TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

KATARIINA KANNUS

# SUOMEN VALMISTAVAN TEOLLISUUDEN KYBERTURVALLISUUDEN TULEVAISUUDENNÄKYMIÄ

Diplomityö

Tarkastajat: FT Marko Helenius, TkT Ilona Ilvonen

Tarkastajat ja aihe hyväksytty Tieto- ja sähkötekniikan tiedekuntaneuvoston kokouksessa 04.01.2017

# TIIVISTELMÄ

**KATARIINA KANNUS**: Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuudennäkymiä
Tampereen teknillinen yliopisto
Diplomityö, 88 sivua, 13 liitesivua
toukokuu 2017
tietotekniikan koulutusohjelma
Pääaine: Pervasive Systems
Tarkastajat: FT Marko Helenius, TkT Ilona Ilvonen
Avainsanat: kyberturvallisuus, tietoturvallisuus, Suomen valmistava teollisuus, valmistava teollisuus, IoT:n turvallisuus, IIoT:n turvallisuus;

Suomen valmistavan teollisuuden kyberturvallisuustoiminta on usein melko reaktiivista. Yleensä vasta vakavat kyberhyökkäykset antavat sysäyksen kyberturvallisuuden kehittämiselle - jolloin saattaa olla jo liian myöhäistä. Tämän työn yhtenä tärkeänä tavoitteena oli auttaa kehittämään Suomen valmistavan teollisuuden kyberturvallisuutta proaktiivisemmaksi selvittämällä sen tulevaisuudennäkymiä.

Näitä tulevaisuudennäkymiä tutkittiin tunnetulla tulevaisuudentutkimusmenetelmällä, delfoilla. Työssä selvitettiin, mikä Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021 on tärkeää ja mikä ei. Samalla työ kartoitti ja loi kuvaa Suomen valmistavan teollisuuden kybertoimintaympäristöstä vuonna 2021.

Tutkimuksessa saatiin selville, että vuonna 2021 Suomen valmistavan teollisuuden kyberturvalle tärkeimpiä asioita ovat todennäköisesti esineiden internet (IoT), teollisuusautomaation turvallisuus, digitalisaatio sekä teollisuuden neljänneksi vallankumoukseksi kutsuttu industry 4.0. Tärkeää tulee olemaan myös identiteettien ja pääsynhallinta sekä saatavuuden varmistaminen. Lisäksi esimerkiksi datan suojaus, vanhojen ja monimutkaisten järjestelmien perintö sekä kyberturvakulttuurin muutos tunnistettiin mahdollisesti tärkeiksi alan kyberturvallisuudelle vuonna 2021.

Kokonaisuutena tämän diplomityön tarkoitus on auttaa kyberturvallisuuden asiantuntijoita ennakoimaan suomalaisen valmistavan teollisuuden kyberturvallisuuden lähitulevaisuuden trendejä ja siten auttaa heitä suunnittelemaan paremmin omaa työtään. Tarkoitus on myös helpottaa strategista päätöksentekoa, kuten investointipäätöksiä, ja tarjota tietoa rajallisten resurssien järkevään kohdentamiseen.

# ABSTRACT

**KATARIINA KANNUS**: The Future Prospects of Cyber Security in Finnish Manufacturing Industry
Tampere University of Technology
Master's Thesis, 88 pages, 13 Appendix pages
May 2017
Master's Degree Programme in Information Technology
Major: Pervasive Systems
Examiner: PhD Marko Helenius, D.Sc. Ilona Ilvonen
Keywords: cyber security, information security, Finnish manufacturing, manufacturing, IoT security, IIoT security;

Cyber security activities among Finnish manufacturing industry companies seem rather reactive. Too often a serious cyberattack is needed to improve and develop organization's cyber security - and by then it can be too late. Therefore, one of the main purposes of this thesis was to make the cyber security management in the Finnish manufacturing industry more proactive by studying its future prospects.

These future prospects were explored by using a commonly known future forecasting method called delphi. The study analysed what are the cyber security priorities among Finnish manufacturing industry in 2021. Simultaneously, the thesis created an image of the Finnish manufacturing industry's cyber environment for 2021.

The thesis found out that internet of things, digitalisation, industry 4.0, and the security of the industrial automation will probably be the most important drivers for the cyber security of Finnish manufacturing industry in 2021. Also, identity and access management as well as ensuring availability will be important. Among other things, data protection, the legacy of old and complex systems, and cyber security culture transformation may be essential themes in industry's cyber security in 2021.

Overall, this study is meant to help cyber security professionals of the Finnish manufacturing industry by driving them to anticipate the future trends in the cyber landscape of the industry. In this way it can be easier for them to plan their future work and priorities. The purpose is also to ease strategic decision-making, such as investment decisions, and offer good knowledge basis for planning reasonable use of limited cyber security resources.

# ALKUSANAT

Tässä diplomityöprosessissa oli apuna ja tukena useita henkilöitä, joita kaikkia haluan kiittää. Mielenkiintoisesta ja haastavasta aiheesta kiitokset ansaitsee työnantajani Deloitte, joka myös mahdollisti hyvät puitteet työn tekemiselle. Erityisesti Deloitten Cyber Risk -tiimille kiitokset avusta, kannustuksesta ja ymmärryksestä. Haluan myös kiittää jokaista yhdeksää tutkimukseen haastateltua asiantuntijapanelistia heidän ajastaan sekä jakamastaan asiantuntemuksesta.

Kaikkein suurin kiitos kuuluu varmasti esimiehelleni ja työn ohjaajalle Tero Mellinille. Ilman hänen ohjaustaan, innostavuuttaan sekä positiivista asennettaan työn tekeminen olisi ollut vähintäänkin haastavaa, ehkä jopa mahdotonta. Lisäksi kiitokset työn tarkastajille Ilona Ilvoselle sekä Marko Heleniukselle heidän neuvoistaan ja tuestaan.

Lopuksi haluan tietenkin kiittää perhettäni ja muita läheisiäni, joiden tuki on ollut korvaamattoman tärkeää koko diplomi-insinööriopintojeni ajan.

Tampereella, 24.5.2017

Katariina Kannus

# SISÄLLYS

# KUVALUETTELO

# TAULUKKOLUETTELO

# LYHENTEET JA MERKINNÄT

| | |
|---|---|
| Bottiverkko | *Botnet*; Jokin tietoverkon, kuten internetin, välityksellä toisiinsa kytkettyjä botteja eli koneita esim. tietokoneita tai IoT-laitteita, jotka voivat olla tarkoitukseen kaapattuja. Bottiverkon tavoitteena voi olla esimerkiksi haittaohjelmien levitys tai hyökkäyksien tekeminen. Bottiverkon ohjaukseen voidaan käyttää hallintapalvelinta tai -sovellusta (*command & control server/software*). |
| Brute-force | Kaikkien mahdollisten ratkaisujen kokeileminen tavoitteena oikean osuminen kohdalle. Brute-force-hyökkäyksessä tietokone tai bottiverkko valjastetaan kokeilemaan kaikki mahdolliset salasanayhdistelmät ja jos oikea osuu kohdalle, hyökkäys onnistuu tavoitteessaan. |
| Delfoi | *Delphi*; Tunnettu, semimäärällinen, systemaattinen, interaktiivinen, iteratiivinen ja strukturoitu tulevaisuudentutkimusmetodi, jossa asiantuntijapaneeli etsii anonyymisti vastausta vai vastauksia asetettuun kiistakysymykseen. |
| DoS | *Denial of Service*; Palvelunesto eli jonkin järjestelmän ylikuormitus, häiritseminen tai haavoittaminen niin, ettei sitä voida käyttää. |
| Eheys | *Integrity*; Tietoturvakontekstissa tarkoittaa tiedon muuttumattomuutta ja oikeellisuutta siten, että tieto ei ole viestityksen tai tallennuksen yhteydessä muuttunut. Tietoturvan tarkoitus on suojata mm. tiedon eheyttä. |
| ENISA | *European Union Agency for Network and Information Security*; Euroopan Unionin erillisvirasto, jonka tehtävänä on parantaa verkko- ja tietoturvallisuutta Unionin alueella. |
| ICS | *Industrial Control System*; Teollisuuden ohjausjärjestelmä, joka kontrolloi ja monitoroi teollisia prosesseja. |
| IIoT | *Industrial Internet of Things*; Teollinen esineiden internet. |
| IoT | *Internet of Things*; Esineiden internet (jossakin lähteissä myös asioiden internet) tarkoittaa fyysisten esineiden yhdistämistä internetverkkoon, joka mahdollistaa mm. niiden etäohjattavuuden sekä yhteydet toisiinsa. |
| IP-data | *Intellectual Property Data*; Immateriaali- ja/tai tekijänoikeuksien alainen pääoma. |
| Kiistakysymys | *Issue*; Kiinnostava, julkinen ja ratkaisematon keskustelun aihe, joka odottaa lähitulevaisuudessa ratkaisua. |

| | |
|---|---|
| Kyberriski | *Cyber risk*; Kybertoimintaympäristöön kohdistuva vahinkomahdollisuus tai haavoittuvuus, joka toteutuessaan tai jota hyväksi käyttäen kybertoimintaympäristön toiminnasta riippuvalle toiminnolle voi aiheutua vahinkoa, haittaa tai häiriötä [2]. |
| Kybertoiminta-ympäristö | *Cyber environment*; Sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö [2]. |
| Kyber-turvallisuus | *Cyber security, myös kyberturva*; Toimenpiteet, joilla organisaatio suojautuu kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteuttaa tarvittavia vastatoimenpiteitä [3], sekä tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan [2]. |
| Kyberuhka | *Cyber threat*; Mahdollisuus sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon [2]. |
| Luottamuksellisuus | *Confidentiality*; Tietoturvakontekstissa tarkoittaa sen varmistamista, että tieto on ainoastaan siihen oikeutettujen käytettävissä. Tietoturvan tarkoitus on suojata mm. tiedon luottamuksellisuutta. |
| Milleniaalit | *Millennials*; Sukupolvi, joka on syntynyt suurin piirtein vuosien 1980-2000 välissä. |
| MItM | *Man-in-the-middle (attack)*; välistävetohyökkäys, jossa hyökkääjä pääsee uhrien välisen tietoliikeenteen välittäjäksi kuuntelemaan tai muuttamaan siinä kulkevia viestejä uhrien huomaamatta. |
| Nollapäivä-haavoittuvuus | *Zero-day vulnerability*; Poulustautujalle ennennäkemätön haavoittuvuus. Jos haavoittuvuutta käytetään hyväksi hyökkäyksessä, puolustautujalle jää haavoittuvuuden nimen mukaisesti nolla päivää aikaa suojata järjestelmänsä haavoittuvuudelta. |
| Ransomware | Kiristyshaittaohjelma, joka ensin estää järjestelmien tai tiedostojen käytön esimerkiksi salaamalla tai lukitsemalla ne ja vaatii sen jälkeen lunnaita niiden avaamisesta. Ransomware-hyökkäys saattaa myös vaatia lunnaita siitä, että uhrilta varastettuja tietoja ei julkaista. |
| Saatavuus | *Availablity*; Kertoo, onko järjestelmä, ohjelma, tieto, laite tai palvelu käytettävissä halutulla hetkellä. Tietoturvallisuuden tarkoitus on suojata mm. tiedon saatavuutta. |
| SCADA | *Supervisory, Control and Data Acquisition System*; Teollisuudessa käytetty käytönohjaus- ja valvontajärjestelmä. |

| | |
|---|---|
| Social engineering | Ihmisten psykologinen manipulointi tekemään jotain, jota he eivät normaalisti tekisi, esimerkiksi vuotamaan sensitiivisiä tietoja. Yleisiä social engineering hyökkäyksiä ovat esimerkiksi tietojenkalastelu ja erilaiset huijaukset. Niissä hyökkääjä käyttää hyväkseen ihmisen luonnollisia reaktioita, tarpeita ja haluja, kuten luottamusta, auktoriteettien kunnioitusta ja miellyttämisen halua. |
| SWOT | *Strength, Weakness, Opportunity, Threat*; Nelikenttäanalyysi, jolla voidaan selvittää yrityksen sisäiset vahvuudet ja heikkoudet sekä ulkoiset tulevaisuuden mahdollisuudet ja uhat. SWOT on yleisesti käytetty yritystoiminnan analysointimenetelmä. [4]. |
| Takaovi | *Backdoor*; Menetelmä, joka mahdollistaa pääsyn suojattuihin tietoihin (esimerkiksi yrityksen verkkoon) ilman yleensä vaadittua todennusta. |
| Tietosuoja | *Privacy and data protection*; Henkilön yksityisyyden suojaaminen oikeudettomalta tai henkilöä vahingoittavalta käytöltä. Tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. [2]. |
| Tietoturvallisuus | *Information Security*; Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. |
| Valmistava teollisuus | *Manufacturing*; Teollisuuden ala, jonka liiketoiminta perustuu jonkin tuotteen tai tuotteiden tuotantoon, tai raaka-aineen tai raaka-aineiden jalostukseen. |

# 1. JOHDANTO

Suomi on yksi kehittyneimmistä digitaalisista tietoyhteiskunnista. Suomen valmistavan teollisuuden yrityksien toiminnot ovat riippuvaisia erilaisista digitaalisista verkoista ja niiden palveluista. Eikä tämä riippuvuus vaikuta tulevaisuudessa ainakaan vähenevän. Kyberturvallisuus on digitalisaation mahdollistaja, mutta huonosti toteutettuna se saattaa viedä kaikki digitalisaation tuomat edut. [5, s. 8, 66].

Kyberhyökkäyksien monimutkaisuus, tehokkuus ja kyvykkyys kasvavat nopeammin kuin organisaatioiden puolustuskyky. Suomalaisissa yrityksissä kyberturvallisuus onkin proaktiivisuuden sijaan edelleen lähinnä reaktiivista ja usein vasta vakavat kyberhyökkäykset antavat sysäyksen turvallisuustoimenpiteiden kehittämiselle. [5]. Tällöin saattaa olla jo liian myöhäistä, sillä kyberhyökkäys on jo voinut vaikuttaa uhriin ja tämän liiketoimintaan. Hyökkääjä on esimerkiksi saattanut varastaa yrityksen tärkeitä tietoja tai pysäyttää tärkeitä toimintoja kuten kokonaisen tehtaan tai sen osan [6, 7, 8]. Näin ollen onnistunut kyberhyökkäys saattaa vaikuttaa ei ainoastaan tietotekniikkaan ja -verkkoihin vaan niiden kautta myös fyysiseen maailmaan ja yrityksien jokapäiväiseen liiketoimintaan.

Proaktiivisen eli ennakoivan kyberturvallisuustoiminnan saavuttamiseksi sekä elinkeinoelämä että muu yhteiskunta tarvitsevat tutkimusta kyberturvallisuuden tulevaisuudesta eri toimialojen näkökulmista. Tässä tutkimuksessa selvitetään kyberturvallisuuden tulevaisuudennäkymiä suomalaisen valmistavan teollisuuden näkökulmasta: mikä sen kyberturvallisuudelle on vuonna 2021 tärkeää, mikä vähemmän tärkeää ja millaista kyberturvallisuutta Suomen valmistavan teollisuuden yritykset ylipäätään tavoittelevat?

## 1.1 Työn taustaa

Tietotekniikan levittäytyminen yhä laajemmin teollisuustuotanto- ja ohjausjärjestelmiin on luonut uusia haavoittuvuuksia ja mahdollisia hyökkäyskohteita valmistavan

teollisuuden kybertoimintaympäristöön [2]. IBM:n kansainvälisen tutkimuksen mukaan valmistava teollisuus olikin vuonna 2015 toiseksi eniten hyöykkäyksiä ja niiden yrityksiä kohdannut toimiala heti terveydenhuollon jälkeen [9] ja edelleen vuoden 2016 raportissa valmistava teollisuus listattiin yhdeksi hyökätyimmistä toimialoista [10]. Tutkimukset perustuvat IBM:n kyberturvallisuuden monitoroinnin asiakkaistaan keräämään dataan. Myös Symantecin raportti *2017 Internet Security Threat Report* [11] kertoo valmistavan teollisuuden olevan kolmanneksi eniten tietomurtoja kohtaava toimiala.

Tutkimusten [12, 13, 14, 15] mukaan kyberturvallisuus ei ole enää vain IT:n tai tietohallinnon huolenaihe, vaan se on nousemassa tärkeiden asioiden joukkoon myös muualla liiketoiminnassa, esimerkiksi yrityksien johdossa. Deloitten *EMEA 360 Boardroom Survey 2016* [15] ennustaa, että jo seuraavan parin vuoden aikana kyberturvallisuus on yksi avainkysymyksistä yrityksien hallituksissa. Samassa tutkimuksessa alle puolet vastaajista sanoi, että heidän yrityksessään on tutkimuksen tekohetkellä kyberturvallisuuden toimintasuunnitelma. Lisäksi 20 %:ssa yrityksistä hallituksen tietoisuus kyberturvallisuudesta arvioitiin alhaiseksi. Tästä huolimatta vastaajien mukaan hallituksen katsotaan olevan lopullisessa vastuussa kyberturvallisuudesta. Tutkimuksessa oli mukana 271 vastaajaa EMEA-alueen (Eurooppa, Lähi-itä ja Afrikka) eri yrityksistä, joista 22 Suomesta. Vastaajista 20 % edusti valmistavan teollisuuden yritystä.

Kansainvälisissä tutkimuksissa [16, 17] on huomattu ristiriita yrityksien ylemmän johdon kyberturvallisuuteen liittyvien odotuksien ja panostuksien välillä - tietohallintojohtajien tiimeineen odotetaan huolehtivan yrityksen kyberturvallisuudesta, mutta siihen ei olla valmiita investoimaan tarpeeksi. Deloitten maailmanlaajuisessa tutkimuksessa [16] 45 % tietohallintojohtajista oli sitä mieltä, että kyberturvallisuudella on suuri merkitys heidän yrityksiensä liiketoimintaan seuraavan kahden vuoden aikana. Samassa tutkimuksessa 41 % tietohallintojohtajista sanoo yrityksensä kyberturvallisuusinvestointien olevan riittämättömiä. Kuitenkin 64 % vastaajista uskoo kyberturvallisuusinvestointien kasvavan kahden vuoden aikana.

On tutkittu, että kyberturvallisuuden unohtaminen käy yrityksille helposti kalliiksi. Muun muassa Ponemon Institute [18] on jo useamman vuoden ajan tutkinut aihetta. Heidän mukaansa tietoturvaloukkaus maksaa yritykselle keskimäärin 4-73 miljoonaa dollaria [19]. Tutkimuksessa oli mukana 383 yritystä 12 eri maasta. Suomi ei kuitenkaan ollut edustettuna. Kuitenkin yhä kansainvälisempi toiminta tuo vas-

taavat kustannukset koskemaan myös suomalaista valmistavaa teollisuutta. Lisäksi on huomattava, että kyberhyökkäyksen kaikki liiketoimintaan vaikuttavat seuraukset eivät ole heti näkyvissä, vaan vaikutukset ovat monimutkaisia ja pidempiaikaisia [20]. Nämä ovat syitä, miksi kyberturvallisuuden tulevaisuutta täytyy tutkia, ei ainoastaan esimerkiksi kansallisen turvallisuuden vaan myös muun muassa yrityksien liiketoiminnan jatkuvuuden näkökulmasta.

Nimenomaan valmistavan teollisuuden kyberturvallisuuden tulevaisuudennäkymien tutkiminen on tärkeää, sillä tiedetään, että alan kybertoimintaympäristö on jatkuvassa muutoksessa (katso esimerkiksi [21], [22], [23] tai [24]). Valmistavan teollisuuden ympäristöjen uudet teknologiat tuovat mukanaan uudenlaisia kyberuhkia samaan aikaan, kun hyökkääjät löytävät aina vain uusia keinoja käyttää hyödyksi vanhojen järjestelmien, teknologioiden ja prosessien haavoittuvuuksia. On helppo päätellä, että hyökkääjien resurssit ovat paitsi suuremmat, myös nopeammin ja helpommin allokoitavissa, kuin heitä vastaan puolustautuvien yrityksien.

Suomen kyberturvallisuusstrategiassa [2] sanotaan: "Kyberuhkien torjunta vaatii hyvää suunnittelua ja ennakointia. Uusi toimintaympäristömme edellyttääkin kaikilta osapuolilta vahvaa osaamista sekä nopeaa, oikean suuntaista ja yhdenmukaista reagointia eli strategista ketteryyttä. Kyberturvallisuuden johtamisessa ilmentyy strategisen ketteryyden kaikki kolme tekijää, joita ovat strateginen herkkyys, johdon yhtenäisyys sekä resurssien joustava käyttö." Näin ollen, aivan kuten ei muidenkaan yrityksen toimintojen, ei kyberturvallisuudenkaan johtaminen voi keskittyä vain nykytilan hallinnoimiseen ja arviointiin, vaan on oleellista ymmärtää ja huomioida myös tulevaisuuden tarpeet sekä trendit. Ymmärtämättä tulevaisuutta ja ennakoimatta trendejä haasteena on esimerkiksi hallita ja hyödyntää resursseja oikea-aikaisesti ja oikealla tavalla, kuten esimerkiksi investoida oikeisiin asioihin oikeaan aikaan.

Vaikka nykypäivän suomalainen valmistava teollisuus on usein edelleen johdettu Suomesta, niin sen liiketoimintaympäristö on yhä kansainvälisempää. Suomalaisilla yrityksillä on yhä enemmän toimintoja, esimerkiksi tehtaita, yhteistyökumppaneita ja asiakkaita, ympäri maailmaa. Tulevaisuudessa yhä globaalimpi toiminta tuo monille suomalaisille valmistavan teollisuuden yrityksille paitsi paljon mahdollisuuksia kasvuun, niin myös erilaisia uusia haasteita. Yksi suuri haaste on juuri kyberturvallisuuden hallinnoiminen ja tulevaisuuden kyberuhkiin varautuminen. Tässä tutkimuksessa keskitytään selvittämään, mitkä kyberturvallisuuden lähitulevaisuuden

kansainvälisistä haasteista koskevat erityisesti Suomen valmistavaa teollisuutta.

## 1.2 Tutkimusongelma ja sen rajaus

Tässä tutkimuksessa selvitettiin suomalaisen valmistavan teollisuuden kyberturvallisuuden tulevaisuudennäkymiä noin 4-5 vuoden aikajänteellä. Vuoteen 2021 ulottuva aikajänne valittiin siksi, että yleensä yritykset suunnittelevat strategiansa ja toimintansa ainakin viisi vuotta eteenpäin. Tutkimuksen tarkoitus oli selvittää, onko tulevaisuuden kyberuhkiin varautuminen sisällytetty näihin suunnitelmiin. Lisäksi suomalaisen valmistavan teollisuuden kyberturvallisuuden kanssa työskenteleviltä kysyttiin, millaiset asiat ovat yrityksien kyberturvallisuudelle tärkeitä vuonna 2021 ja miksi.

Monet asiantuntijat teollisuuden tuotantolaitoksissa sekä automaatiotoimittajien puolella ovat tunnistaneet tieto- ja kyberturvallisuuden merkityksen teollisuusautomaation ylläpidossa [25]. Tässä tutkimuksessa selvitettiin, alkaako tämä näkyä tulevaisuudessa konkreettisina toimenpiteitä - esimerkiksi kyberturvallisuuteen kohdistettuina investointeina tai riittävinä resursseina.

Kyberturvallisuudesta on monenlaisia määritelmiä. Tässä tutkimuksessa kyberturvallisuutta lähestyttiin samalla määritelmällä kuin Lehto ja Kähkönen raportissaan *Kyberturvallisuuden kansallinen osaaminen* [3]. He määrittelevät kyberturvallisuuden toimenpiteiksi, joilla organisaatio suojautuu kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteuttaa tarvittavia vastatoimenpiteitä. Heidän mukaansa kyberturvallisuusstrategian ja -ohjelman rakenne ja elementit riippuvat organisaation arvioiduista uhkatekijöistä ja riskeistä. Näin ollen kyberturvallisuuden pohjana on organisaation riski- tai uhka-analyysi.

Kyberturvallisuuden määritelmä ei kuitenkaan ole yksinkertainen tai aina samalla tavalla ymmärretty. Esimerkiksi edellisestä hieman eroava näkökulma kyberturvallisuuteen on määritelty Suomen kyberturvallisuusstrategiassa [2]: "Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan." Tähän tutkimukseen osallistuneilta asiantuntijoilta kysyttiinkin, mitä kyberturvallisuus heidän mielestään on. Tällöin haastattelujen osapuolien oli helpompi varmistua siitä, että puhuttiin samasta asiasta.

Tässä tutkimuksessa selvitettiin, millaisia ovat suomalaisen valmistavan teollisuuden näkökulmasta tärkeimmät sen kyberturvallisuuden lähitulevaisuuteen vaikutta-

vat asiat. Tämä tutkimuksen tarkastelun ulkopuolelle jätettiin teollisuuden järjestelmien teknisiä ongelmia, joita voidaan yleensä pitää sisäisinä heikkouksina. Yleisesti riskienhallinnasta tunnetun SWOT-nelikenttäanalyysin [4] mukaisesti kyberuhkaa käsiteltiin siis ulkoisena uhkana. Tällöin järjestelmien sisäisistä heikkouksista katsottiin tulevan ulkoisia uhkia ainoastaan silloin, kun ulkopuolisen hyökkääjän on mahdollista käyttää niitä hyväkseen pahantahtoisissa toimissaan. Näin ollen esimerkiksi tahattomasta ohjelmointivirheestä johtuvaa tuotantokoneen seisahtumista ei katsottu tässä työssä kyberuhkaksi, vaikka se onkin uhka yrityksen liiketoiminnalle ja tietoturvanäkökulmasta uhka esimerkiksi saatavuudelle.

Yksi tämän tutkimuksen tarkemmista tutkimuskysymyksistä oli, kuinka tutkimuksen kohdeyrityksissä oli tällä hetkellä investoitu kyberturvallisuuteen ja kuinka siihen aiottiin investoida tulevina vuosina, 1-5 vuoden aikajänteellä. Investoinnit luovat kuvaa yrityksen tulevaisuudennäkymistä, jolloin niiden oletetaan aloittavan maksaa itseään takaisin. Kuitenkin kyberhyökkäyksien väitetään tuplaantuneen viiden vuoden aikana joka vuosi, kun taas samalla ajanjaksolla kyberturvallisuusbudjetit ovat suurentuneet alle 20 % [5].

## 1.3 Työn toteutus

Työn merkittävin saavutus on sen luoma näkemys Suomen valmistavan teollisuuden kyberturvallisuudesta vuonna 2021. Näkemys luotiin ensisijaisesti tulevaisuudentutkimuksessa paljon käytetyllä delfoi-tutkimusmenetelmällä sekä sitä pohjustavalla kirjallisuuskatsauksella. Delfoita varten Suomen valmistavan teollisuuden yrityksistä koottiin asiantuntijapaneeli, jonka jäsenet olivat kyseisten organisaatioiden kyberturvallisuus-, tietoturva-, turvallisuus- tai tietohallintojohtajia.

Tutkimukseen osallistuneet yritykset valikoitiin seuraavin kriteerein:

- edustaa valmistavaa teollisuutta
- pääkonttori ja suurin osa IT-johdosta Suomessa
- edustettuna Talouselämä 500 2016 -listalla [26]
- edustettuna Kauppalehden Tuloksentekijät-listalla 20.10.2016 [27]
- vuoden 2015 liikevaihto 84 - 12 500 milj. euroa (8:lla yrityksistä yli 1500 milj. euroa ja 5:llä yrityksistä yli 5000 milj. euroa)

- globaalia toimintaa (esim. globaaleja asiakkaita ja/tai tehtaita ulkomailla)

Yllä listattujen lisäksi tutkimukseen valituissa yrityksissä oli yleisesti käytössä hajautettuja järjestelmiä ja niissä oltiin kiinnostuneita käyttämään tai käytettiin jo IoT:n tai teollisen internetin ratkaisuja. Lisäksi yrityksessä tietenkin täytyi olla asiantuntijapanelistiksi sopiva henkilö, jolla on tarpeeksi näkemystä kyberturvallisuuden hallinnasta paitsi omassa organisaatiossaan niin myös alalla yleisesti.

Delfoista käytettiin versiota, jossa panelisteja haastateltiin yksitellen kaksi kertaa: ensimmäisellä iteraatiokierroksella paneeli ensin tutustutettiin aiheeseen etsien samalla ensimmäisiä hypoteeseja ja väittämiä Suomen valmistavan teollisuuden kyberturvallisuudelle tärkeistä asioista vuonna 2021. Toisella iteraatiokierroksella panelistit syventyivät ensimmäiseltä kierrokselta esille nousseisiin asioihin ja argumentoiden kommentoivat sekä omiaan että muiden panelistien mielipiteitä.

Delfoi-menetelmään päädyttiin, sillä se on paljon käytetty menetelmä erityisesti tulevaisuudentutkimuksessa. Delfoi on vanha menetelmä, jonka juuret ulottuvat antiikin Kreikkaan. Ominaisuuksiensa puolesta delfoin sopii anonyymisti toisilleen näyttäytyvän asiantuntijaryhmän kommunikaatioprosessin strukturointiin. Tarkoituksena on, että eri orientaation omaavat yksilöt käsittelevät monimutkaista ongelmaa ryhmässä argumentoiden. [28, 29, 30, 31]. Menetelmä soveltuu siis hyvin kyberturvallisuuden tulevaisuuden tutkimiseen, sillä delfoi takaa asiantuntijapanelisteille vapaan mahdollisuuden keskustella aiheesta anonyymisti.

Delfoita käytetään, kun halutaan etsiä asiantuntijaryhmän avulla vastausta monimutkaiseen kiistakysymykseen. eDelfoi-sivusto [28] määrittelee ihanteellisen kiistakysymyksen olevan "kiinnostava, julkinen ja ratkaisematon keskusteluaihe, joka odottaa lähitulevaisuudessa ratkaisuaan". Delfoin käyttö on suosittua etenkin silloin, kun halutaan selvittää, mitkä asiat tarvitsevat lähempää tutkimusta, tai kun halutaan rajata tutkimusaluetta tai hakea ennakoinnin suuntaa. Tässä tutkimuksessa kiistakysymys oli sama kuin tutkimusongelma, eli tarkoitus oli selvittää alan asiantuntijoiden näkemyksiä suomalaisen valmistavan teollisuuden kyberturvallisuudesta vuonna 2021.

Delfoi luokitellaan semimäärälliseksi tutkimusmenetelmäksi. Tämä tarkoittaa, että kvalitatiiviseen eli laadulliseen tutkimukseen lisätään kvantitatiivisia eli määrällisiä elementtejä. [30]. Lisäksi delfoi luokitellaan asiantuntijamenetelmäksi. Asiantuntijamenetelmiä käytettäessä ratkaisevaa ei ole asiantuntijoiden määrä vaan laatu. [29].

Yhdeksän asiantuntijaa on järkevä paneelin koko työn laajuuteen nähden ja toisaalta riittävä tutkimuksen tavoitteita ajatellen.

Esimerkki isosta delfoi-paneelista ja tutkimuksesta on YK-yliopiston Millenium-projekti. Se on yksi luultavasti kuuluisimmista ja mittavimmista delfoi-menetelmän sovellutuksista. Siinä kansainvälinen asiantuntijapaneeli arvioi tulevaa maailmanlaajuista kehitystä. [29]. Suomessa delfoilla on tutkittu muun muassa kansallisten turvallisuustoimijoiden yhteistyötä [32] sekä kilpailun kehitystä Euroopan energiamarkkinoilla [33].

Seuraavassa luvussa 2 lukija perehdytetään diplomityön aiheeseen esittelemällä tämän työn aiheen ja tavoitteiden kannalta kiinnostavimpia ja tuoreimpia kyberturvatutkimuksia eri puolilta maailmaa. Tämän jälkeisessä luvussa 3 tutustutaan tarkemmin tutkimusmenetelmä delfoihin sekä tämän tutkimuksen kulkuun: delfoin valmisteluun sekä molempiin haastattelukierroksiin. Seuraavassa luvussa 4 kootaan yhteen delfoin tulokset sekä verrataan niitä lyhyesti luvun 2 kirjallisuuskatsaukseen. Viimeisessä luvussa 5 palataan vielä tutkimuksen tärkeimpiin tuloksiin, pohditaan tutkimuksen onnistumista sekä jatkotutkimustarpeita.

# 2. KATSAUS MUIHIN KYBERTURVATUTKIMUKSIIN

Tämän tutkimuksen pohjaksi tehtyyn kirjallisuuskatsaukseen valittiin tutkimuksen tavoitteiden kannalta kiinnostavimmat aiheesta aikaisemmin tehdyt tutkimukset ja raportit. Tärkeimpänä kriteerinä katsaukseen otetulle kirjallisuudelle oli lopulta sen tuoreus: valitut tutkimukset ja raportit olivat muutaman viime vuoden ajalta, vanhimmat vuodelta 2015. Rajaus tehtiin vuoteen 2015, sillä kyberturvallisuudelle on luonteenomaista jatkuva sekä tietyillä toimialoilla, kuten valmistavassa teollisuudessa, myös erittäin nopea, muutos. Tällöin jo muutamankin vuoden vanhojen tutkimuksien ja raporttien voidaan katsoa olevan vanhentuneita - erityisesti, kun tarkoituksena on tutkia alan tulevaisuutta 4-5 vuoden aikajänteellä.

Katsauksessa haettiin ensisijaisesti juuri Suomea ja sen valmistavaa teollisuutta koskevaa kirjallisuutta. Lopulta kirjallisuuskatsaus ulotettiin kuitenkin myös aiottua enemmän ulkomaisiin lähteisiin, koska aiheesta on julkaistu Suomessa hyvin vähän viime vuosina mitään, missä juuri valmistavan teollisuuden kybertoimintaympäristöön liittyvät asiat olisivat mukana. Lisäksi ulkomaisen kirjallisuuden mukaan ottaminen oli perusteltua, koska Suomen valmistavan teollisuuden yrityksien koko toimintaympäristö on nykyään hyvin globaalia. Huomioitavaa kuitenkin oli, että Suomea tai etenkään sen valmistavaa teollisuutta ei aina oltu sisällytetty ulkomaalaisten raporttien tai tutkimuksien laajuuteen, mistä toki oli poikkeuksia, erityisesti eurooppalaisessa tutkimuksessa.

Kirjallisuuskatsaukseen käytettiin sekä Deloitten että Tampereen teknillisen yliopiston (TTY) työntekijöilleen ja opiskelijoilleen tarjoamia tietokantoja. TTY:n tietokannoista oli käytössä kirjaston tietokanta (http://www.tut.fi/fi/kirjasto/). Näistä tietokannoista tehtiin hakuja systemaattisesti aiheeseen liittyvillä hakusanoilla ja hakusanayhdistelmillä suomeksi ja englanniksi. Käytettyjä hakusanoja olivat muun muassa *kyberturvallisuus, tietoturva, kyberturvallisuuden tulevaisuus, kyberturvallisuuden ennakointi, turvallisuuden ennakointi, valmistavan teollisuuden tulevaisuus,*

*valmistava teollisuus muutoksessa, esineiden internetin turvallisuus, teollisen internetin tulevaisuus, teknologian ennakointi* sekä näiden englanninkielisiä versioita kuten *the future of manufacturing, cyber security predictions, Security of Internet of Things, Information Security in Industrial Internet, the future of IoT* ja niin edelleen. Lisäksi koko diplomityöprosessin ajan, erityisesti sen alkuvaiheessa, seurattiin Viestintäviraston Kyberturvallisuuskeskuksen (*https://www.viestintavirasto.fi/kyberturvallisuus.ht* viestintää, jolloin mukaan oli mahdollista saada tuoreinta kirjallisuutta aiheesta.

Kansainvälistä tutkimusta tieto- sekä kyberturvallisuudesta on viimeaikoina tehty paljon. Suomalaisista yrityksistä tutkimusta on tehty selvästi vähemmän, erityisesti yksityisen puolen organisaatioiden näkökulmasta. Suurin osa suomalaisiin yrityksiin kohdistuvista tutkimuksista näyttää keskittyvän organisaatioiden kyberturvallisuuden nykytilaan, ei niinkään tulevaisuuteen. Lisäksi tutkimuksissa on mukana yleensä yksityisen sektorin yritysten ohella julkisen puolen organisaatioita. Esimerkkejä tällaisesta kirjallisuudesta viime vuosilta ovat muun muassa CGI:n teettämä *Kyberturvallisuus digitalisoituvassa maailmassa* -tutkimus [34] sekä Viestintäviraston Kyberturvallisuuskeskuksen vuosiraportit [35, 36].

Aiempia julkaisuja erityisesti Suomen valmistavan teollisuuden kyberturvallisuudesta ja sen tulevaisuudesta ei juuri ole. Yksi julkaisu on kuitenkin Suomen Automaatioseuran turvallisuusjaoston vuonna 2005 teettämä kirja *Teollisuusautomaation tietoturva* (verkkopainos saatavilla [37]). Sen on kirjoittanut suuri joukko alan asiantuntijoita ja se käsittelee monia tämänkin päivän valmistavalle teollisuudelle edelleen ajankohtaisia uhkia. Kirjallisuuskatsaukseen sitä ei kuitenkaan sisällytetty, sillä se on tämän työn kirjoittamishetkellä yli 11 vuotta vanha.

Ulkomailla kyberturvallisuuden tulevaisuutta ennakoiva tutkimus on keskittynyt usein Pohjois-Amerikan markkinalle. Jonkin verran tutkimuksia on tehty myös Euroopan alueella, viime vuosina niitä on julkaissut muun muassa ENISA (The European Union Agency for Network and Information Security) [38, 39, 40]. Kuitenkin myös ENISAn tutkimus näyttää keskittyvän lähinnä kyberturvallisuuden tilaan tällä hetkellä ja lähimenneisyydessä.

Toinen Euroopan tasolla tutkimusta kyberturvallisuuden tilasta tekevä organisaatio on Europolin EC3 (European Cybercrime Centre). Se julkaisee vuosittain IOCTA (Internet Organised Crime Threat Assessment) [41] nimisen raporttinsa kyberrikollisuuden uhkista, jossa on myös lyhyesti käsitelty tulevaisuuden kyberturvallisuuden uhkia ja kehitystä.

Euroopan ulkopuolella, esimerkiksi Pohjois-Amerikassa, tutkimusta kyberturvallisuuden alalta ovat viime aikoina tehneet

- isot kyber- ja tietoturvallisuuspalveluja tai tuotteita tarjoavat yritykset (esim. AT&T [42], Deloitte [20], IBM [43], Kaspersky [44], PwC [45] ja Verizon [6]),
- erilaiset tietoturvatoimijoiden foorumit ja yhdistykset (esim. [46, 12]),
- riippumattomat tutkimusorganisaatiot kuten eri yliopistot (esim. [47] ja [48]), Gartner [49] ja Forrester (esim. [50]).

Seuraavassa luvussa on tämän kirjallisuuskatsauksen osana lyhyesti pohdittu nykypäivän kyberturvakirjallisuutta ja -viestintää sekä lukijan lähdekritiikin merkitystä erityisesti kyberturvallisuuskirjallisuutta tutkiessa.

## 2.1 Pohdintaa nykypäivän kyberturvakirjallisuudesta

On huomattava, että edellä esitellyt kyberturvakirjallisuuden lähteet ovat kaikki erilaisia ja niistä jokaisella on omat, erilaiset syynsä kyberturvallisuustutkimuksen tekemiseen. Varsinkin kaupallisten toimijoiden raportteja ja muita tutkimuksia lukiessa on noudatettava huolellista lähdekritiikkiä ja pidettävä mielessä, miksi raporttiin on kirjoitettu tietyt asiat ja erityisesti, mitä siitä saattaa olla jätetty pois.

Tekstin tyyliin kannattanee myös kiinnittää huomiota: harmittavan yleistä kyberturvakirjallisuudessa sekä muussa kyberturvaviestinnässä tuntuu olevan lukijan pelottelu erilaisilla kauhukuvilla esimerkiksi siitä, kuinka valtavan paljon erilaisia kyberuhkia ja -ongelmia ympärillämme on. Usein tuntuu, että hyödyllisempää olisi kertoa, miten lukija voi ratkaista esitetyt ongelmat käytännössä.

Toki yleisön pelottelullekin on paikkansa ja aikansa esimerkiksi lukijan herättelemissä, mutta enemmän yleiseen turvallisuuteen saattaisi vaikuttaa viestinnän muuttaminen ratkaisukeskeisemmäksi ja jopa positiivisemmaksi. Toisaalta se on kulttuurikohtaista, millainen viestintä saa ihmiset ja heistä koostuvat organisaatiot toimimaan turvallisemmin nykypäivän kyberympäristössä - joskus pelottelu saattaa olla paras keino vaikuttaa.

Tämä tutkimus on valitettavasti yksi niistä, jonka tavoitteisiin ei kuulunut ratkaisujen etsiminen työssä tunnistettuihin ja vielä ratkaisemattomiin kyberturvallisuusongelmiin. Työn laajuuden rajoissa ratkaisujen esittäminen ei ollut mahdollista, sillä ne eivät aina ole tämän tutkimuksen tavoin toimialakohtaisia vaan ennemminkin yrityskohtaisia - tai jopa yrityksen ala-kulttuurikohtaisia. Jokaisen Suomen valmistavan teollisuuden yrityksen on kuitenkin tärkeää huolellisesti suunnitella ja lähteä toteuttamaan omaa kyberturvallisuustoimintaansa enemmän kuin yhden vuoden eteenpäin esimerkiksi tässä tutkimuksessa tunnistettujen asioiden perusteella.

Kyberturvallisuusraporttien sisältöön ja luotettavuuteen vaikuttanee paljon myös se, kenelle se on kirjoitettu. Esimerkiksi kirjallisuuden sisältö saattaa vaihdella hyvin paljon sisällöltään ja tavoitteiltaan riippuen siitä, onko se kirjoitettu raportin tekijöiden asiakkaille, akateemiselle yhteisölle vai poliittisille elimille. Lisäksi tietenkin kirjoittajan tai kirjoittajien henkilökohtainen arvopohja sekä kulttuuritausta toki vaikuttavat, kuten myös ympäristö esimerkiksi oman organisaation arvot. Voikin sanoa, että kuten kyberturvakulttuuri myös kyberturvatutkimuksen kulttuuri tuntuu vaihtelevan esimerkiksi maantieteellisesti tai organisaatiokohtaisesti.

On kuitenkin selvää, että esimerkiksi turvallisuusmonitorointipalveluja tarjoavat yritykset haluavat raporteissaan ja tilastoissaan kertoa, että heidän palvelunsa ovat asiakkaille ja raportin lukijoille tarpeellisia, koska he huomaavat paljon vakavia hyökkäyksiä asiakkaidensa verkkoihin. Kyberturvallisuustutkimuksia leimaakin usein muutaman kyberturvallisuuden osa-alueen pitäminen muita tärkeämpinä, mikä toki on selitettävissä paitsi eri organisaatioiden ja kirjoittajien tavoitteilla niin myös heidän tiedoillaan.

Kyberturvallisuusraportteja tutkiessa on hyvä kiinnittää huomiota tutkimuksen toteutustapaan sekä siihen, kuinka mitäkin asiaa lukijalle korostetaan - mikä toki on hyvä yleisohje minkä vain tutkimuksen lukijalle, myös tämän. Luotettavimpina kirjallisuuskatsauksen lähteinä voinee pitää riippumattomia organisaatiota, sillä niissä kirjoittajan tai kirjottajien tarve on yleensä lähinnä todistaa tutkimuksensa akateeminen merkittävyys, eikä niinkään myydä jotakin ajatusta tai palvelua esimerkiksi pelottelemalla lukijaa tai kertomalla vain tiettyjä tutkimuksessa esille tulleita asioita.

Seuraavassa on esitelty tämän tutkimuksen teemojen ja tavoitteiden kannalta mielenkiintoisimpien julkaisujen näkemyksiä sekä Suomesta että maailmalta. Myös tässä katsauksessa esiteltyyn kirjallisuuteen on syytä suhtautua kriittisesti, sillä esimer-

kiksi kaupallisien toimijoiden esille tuomat luvut voivat hyvinkin olla oikein, mutta niiden esitystapa saattaa olla skandaalinhakuinen. Julkisen sektorin julkaisut vaikuttavat yleensä olevan kaupallisia neutraalimpia, mutta niissäkin voidaan johtaa lukijaa haluttuun suuntaan varsinkin, jos teksti on tarkoitettu poliittisille tai yksityisille päättäjille. Seuraavissa luvuissa esitelty kirjallisuus sisältää hyvin erilaisia tutkimuksia ja lähdekritiikki niitä kohtaan on tässä hieman poikkeuksellisesti jätetty suurissa määrin lukijalle, jonka oletetaan ymmärtävän erilaisten julkaisijoiden motiivit.

## 2.2 Kyberturvan tutkimusta Suomesta

Suomessa kyberturvallisuuden nykytilan tutkimusta tekevät erilaiset riippumattomat organisaatiot kuten yliopistot, ammattikorkeakoulut ja VTT (Valtion teknillinen tutkimuslaitos) [51, 52, 3] sekä erilaiset kaupalliset toimijat kuten kyberturvallisuuskonsultointia ja muita kyberturvallisuuspalveluja tarjoavat yritykset. Lisäksi kuten ulkomailla niin myös Suomessa kyberturvallisuustoimijat tekevät raportteja vuosittaisesta toiminnastaan ja vuoden aikana havaitsemistaan suurimmista ongelmista.

Hyvä esimerkki vuosittaisesta raportista on Viestintäviraston Kyberturvallisuuskeskuksen vuosiraportit [35, 36]. Kyseisissä raporteissa nostetaan esille sekä viisi yleisintä kansalaisen kyberturvallisuusuhkaa että myös viisi yleisintä organisaatioiden uhkaa. Vuoden 2016 tammikuussa julkaistussa raportissa [35] yleisimmäksi uhkaksi organisaatioille nostetaan päivittämättömät ohjelmistot ja toiseksi yleisimmäksi henkilöstön osaamattomuus. Loput kolme ovat järjestyksessä: palvelunestohyökkäykset, huijausviestit ja tietojenkalastelu sekä hallitsemattomat yhteydet sisäverkkoon.

Samat teemat toistuvat viimeisimmässä, vuoden 2017 tammikuussa julkaistussa raportissa [36]. Edellä mainittujen lisäksi listalle ovat nousseet kiristyshaittaohjelmat sekä ulkoisten laitehankintojen hallinta. Hallitsemattomat yhteydet sisäverkkoon -kohta ei enää ole listalla kuten ei myöskään henkilöstön osaamattomuus. Parhaana suojana kyberturvallisuusuhkia vastaan viestintävirasto kuitenkin mainitsee tarkkaavaiseksi koulutetun henkilökunnan.

Monet viestintäviraston tietoon vuonna 2015 tulleet palvelunesto- tai tietojenkalasteluhyökkäykset eivät kuitenkaan ole kohdistuneet valmistavaan teollisuuteen vaan esimerkiksi pankki- ja vakuutusalan yrityksiin [35]. Haittaohjelmat sen sijaan ar-

vioidaan raportissa vakavaksi uhkaksi sekä vakoilun että tuotteen tai palvelun haavoittuvuudesta johtuvien maineongelmien takia. Myös palvelujen saatavuus, kiristäminen sekä internetsivujen valjastus haittaohjelmien levitykseen arvioidaan suomalaisia organisaatioita haittaaviksi uhkiksi. Viestintäviraston raportissa mainitaan myös yhä kehittyneemmät kohdistetut haittaohjelmahyökkäykset, joiden arvioidaan muun muassa vaikuttavan yrityksen kilpailukykyyn haittaavasti tai toimivan väliresurssina tiedonhankinnassa ja arvoketjun osiin vaikuttamisessa. [35].

Sama vuonna 2016 julkaistu raportti [35] katsoo myös hieman tulevaisuuteen ja ennustaa, että kiristyshaittaohjelmien leviäminen yksityisten henkilöiden ongelmasta suomalaisten organisaatioiden ongelmaksi on vain ajan kysymys. Organisaatioiden kiristämiseen on jo nyt käytetty palvelunestohyökkäyksiä, jotka arvioidaan vakavaksi uhkaksi palvelujen saatavuuden ja imago-ongelmien takia. Viestintävirasto ennustaa palvelunestohyökkäyksien hyökkäysvolyymien kasvavan yhä lisää verkkolaitteiden lisääntyessä.

Maailmalla näiden ennakointien on jo nähty toteutuvan: esimerkiksi IBM X-Forcen Yhdysvalloissa teettämän kyselytutkimuksen [43] mukaan kiristyshaittaohjelmat ovat kasvaneet isoksi ongelmaksi myös organisaatioissa ja valitettavasti yrityksien maksaessa lunnaita siitä on tullut myös kannattava tulonlähde verkkorikollisille. Myös palvelunestohyökkäyksien hyökkäysvolyymien kasvaminen on jo käynyt toteen [53].

Viestintäviraston vuonna 2016 julkaisema raportti [36] nostaa myös esille esineiden internettiin liittyvät uhkat. Niistä vakavimmaksi yrityksiä koskevaksi uhkaksi Viestintävirasto arvioi takaoven yrityksen verkkoon ja tietoihin. Lisäksi haittaaviksi uhkiksi raportti luettelee ilkivallan aiheuttamat rahalliset vahingot sekä laitteista saatavat tiedot yritysverkkoon pääsemiseksi.

Suomalaisen valmistavan teollisuuden näkökulmasta kiinnostava on Kyberturvallisuuskeskuksen projekti, jossa kevään 2015 aikana suomalaisesta verkosta löydettiin tuhansia suojaamattomia automaatiolaitteita. Projektin raportti [35] ennakoi muun muassa, että vuonna 2016 esineiden internetin yleistyessä sitä käytetään hyökkäyksiin vielä entistä enemmän. Raportti myös arvelee, että kiinnostus hyökkäyksien kohdistamiseen virtuaaliympäristöihin ja pilvipalveluihin saattaa kasvaa jo vuonna 2016. Myös vuonna 2016 Viestintävirasto teki samanlaisen kartoituksen [54] ja sai samanlaiset tulokset kuin vuonna 2015: suomalaisissa verkkoalueissa on edelleen paljon suojaamattomia automaatiolaitteita.

Viestintävirasto arvioi vuonna 2017 julkaistussa raportissaan [36] nettihuijaukset ja tietojenkalastelun vakavaksi uhkaksi yrityksien maksuliikenteelle. Lisäksi Viestintävirasto luokittelee kiristyshaittaohjelmat edellisen vuoden tapaan vakavaksi uhkaksi, joka uhkaa paitsi yrityksen mainetta, myös palvelujen saatavuutta. Samoja haittoja on muistakin haittaohjelmista ja haavoittuvuuksista, ja niitä voidaan käyttää myös verkkosivujen valjastamiseen haittaohjelmien levitykseen sekä vakoiluun. Vuoden 2017 ilmiöksi Viestintävirasto ennustaa muun muassa mobiililaitteiden tietoturvaheikkoudet. Raportin mukaan vuoden 2017 aikana tullaan näkemään yhä laajempia ja kehittyneempiä mobiililaitteille suunnattuja haittaohjelmakampanjoita.

Vuonna 2017 julkaistussa raportissaan [36] Viestintävirasto on nostanut vakoilun omaksi luvukseen. Siinä vakavaksi uhkaksi nostetaan erilaisten tietojen, kuten innovaatioiden, asiakastietojen tai kilpailutuksien vuotaminen vakoilijoille, jolloin vaikutukset näkyvät kilpailutusten epäonnistumisissa ja tuotekilpailussa. Näissä hyökkäyksissä käytettyjen haittaohjelmien ja työkalujen kehityksen Viestintävirasto ennakoi jatkuvan ja esimerkiksi haittaohjelmista ennustetaan tulevan entistä vaikeammin havaittavia. Yksi kehityssuunnista on muistinvaraiset haittaohjelmat, jotka eivät jätä jälkiä kohdejärjestelmän levyjärjestelmään. Viestintävirasto ennustaa verkkovakoilun lisääntyvän vuoden 2017 aikana ja katsoo sen havaitsemisen organisaatioissa olevan edelleen heikkoa.

Vuoden 2016 yhdeksi ilmiöksi Viestintävirasto nimeää palvelunestohyökkäykset, joita nähdään nyt jo Suomessa päivittäin. Palvelunestohyökkäyksien volyymien ennakoidaan kasvavan lähitulevaisuudessa entisestään ja muun muassa siksi ne kehotetaan ottamaan huomioon yrityksen riskiarviossa. Tähän Viestintävirasto liittää myös esineiden internetin eli IoT:n sekä vakavan uhkan, että organisaatioiden toimintaa tullaan häiritsemään palvelunestohyökkäyksillä, joihin osallistuu IoT-laitteita. Myös rahan kiristäminen palvelunestohyökkäyksellä Viestintävirasto näkee organisaatioita haittaavana uhkana. [36].

Edellisten lisäksi Viestintävirasto [36] ennustaa, että vuonna 2017 tietoturvan merkitys liiketoiminnalle ymmärretään entistä paremmin ja tietoturvaosaamisen kysyntä kasvaa. Tämän Viestintävirasto uskoo johtavan siihen, että tarjonta ei pysy kysynnän perässä ja tietoturvaosaamisesta tulee Suomessakin pulaa. Myös kyberrikollisuuden ammattimaistumisen sekä kaupallistumisen Viestintävirasto ennakoi jatkuvan vuonna 2017.

Hieman pidemmälle tulevaisuuteen katsovaa suomalaista tutkimusta kyberturvalli-

suudesta edustaa vuoden 2017 alussa julkaistu tutkimus *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi* [5]. Osana kyseistä tutkimusta määritellään tavoitetila, jonka mukaan "vuonna 2020 Suomessa kyberturvallisuus on digitaalisen yhteiskunnan sisäänrakennettu ominaisuus, mikä mahdollistaa kaikkien toimijoiden luotettavasti hyödyntää yhteiskunnan kaikkia digitaalisia ratkaisuja turvallisesti".

Samassa tutkimuksessa [5] analysoidaan myös suomalaisen yksityisen sektorin huoltovarmuusyrityksien vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia. Suomalaisten yritysten kyberturvallisuuden johtamisen vahvuuksiksi tunnistetaan seuraavia: kyberturvallisuus on huomioitu strategisena tavoitteena ja politiikka on usein julkaistu; tärkeimmät uhat on tunnistettu; johtaminen on riskiperusteista; kyberturvallisuus on osa kokonaisturvallisuutta ja liiketoimintaa; sekä toimenpiteitä on laitettu tärkeysjärjestykseen. Toisaalta taas johtamisen heikkouksiksi tutkimuksessa luetellaan seuraavia: politiikan jalkautus organisaation läpi, vaativimpia uhkakuvia ei ole tunnistettu, henkilöstön roolitus on usein haastavaa eikä informaatioturvallisuudesta vastaavaa henkilöä ole johtoryhmässä. Lisäksi kyberturvallisuustoiminta on tutkimuksen mukaan edelleen reaktiivista. Tutkimuksessa kuitenkin todetaan, että kaikilla päätöksentekotasoilla on otettu merkittäviä edistysaskelia kohti proaktiivista toimintaa.

*Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi* -tutkimuksessa [5] suomalaisten huoltovarmuusyrityksien vahvuuksiksi tilannekuvan muodostamisessa mainitaan muun muassa uhkatietojen saanti suoraan toimintaverkostosta ja kumppaneilta. Lisäksi vahvuuksiksi nostetaan joidenkin yrityksien ympärivuorokautisen valvonnan sekä Kyberturvallisuuskeskuksen tiedotteet. Heikkouksiksi tilannekuvan muodostamisessa tutkimuksessa luetellaan kuitenkin hajallaan olevat tiedot, toimintaverkoston tilannekuvan hankalan muodostamisen ja IT-varantojen ja automaation (ICS) reaaliaikaisen tilannekuvan puuttumisen. Toisaalta taas hieman vanhempi, vuonna 2014 julkaistu *Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma* väittää, että yrityksien tieto omasta tietoturvastaan on usein puutteellinen [55].

Henkilöstön osaamisesta tutkimuksessa [5] nostetaan suomalaisten yrityksien vahvuuksiksi muun muassa IT-henkilöstön hyvän osaamisen sekä verkkokoulutukset muulle henkilöstölle. Sen sijaan haasteita nähdään koko henkilöstön kouluttamisessa sekä IT/ICS-kokonaisuuden osaamisessa. Jatkuvuuden varmistamisen vahvuute-

na mainitaan laaditut varautumissuunnitelmat sekä harjoitustoiminnan.

Tuotteiden ja palvelujen näkökulmasta vahvuuksiksi tutkimuksessa [5] tunnistetaan muun muassa parhaiden tuotteiden käytön sekä hajautetusti ulkoistetut ostopalvelut. Toisaalta heikkouksiksi luetellaan kumppaniverkoston toiminnan auditoinnin, puutteellisen näkymän palvelujen suojaukseen ja kattavan tunnistautumisen puutteen. Sidosryhmien suhteen positiivisiksi asioiksi listataan muun muassa parhaiden ulkoistuskumppaneiden käytön, toimiala-, viranomais- ja kansainvälisen yhteistyön, sekä yritysten hyvän maineen sidosryhmien keskuudessa. Toisaalta osalle toimialoista tunnistetaan heikkoutena yhteistyömahdollisuuksien puuttuminen. Lisäksi yhtenä heikkoutena mainitaan haasteet liiketoiminnan ja kansallisen huoltovarmuuden yhteensovittamisessa.

Asiantuntijapalveluiden suhteen vahvuuksiksi tutkimuksessa [5] nähdään parhaiden käytäntöjen, standardien ja erilaisten auditointikäytänteiden käyttäminen. Osa tutkimuksen yrityksistä on myös mukana tutkimusohjelmissa. Toisaalta taas yrityksien omaehtoinen tutkimustoiminta on vähentynyt ja koulutuspalvelujen saatavuudessa on tunnistettu haasteita. Lisäksi nähdään puutteita auditoinnin kattavuudessa.

Kyberluottamukseen vaikuttavista uhkatekijöistä tutkimuksessa [5] listataan muun muassa seuraavia: toimintaympäristön analysointi, johon liittyvät sekä tuntemattomat uhkatekijät ja tietomurrot että uudet liiketoimintamallit ja niiden edellyttämiä uusien tekniikoiden käyttöönotto. Uusia tekniikoita ovat muun muassa IoT tai robotiikka, joiden mukana tuomia uhkakuvia ei tutkimuksen mukaan tunneta riittävästi.

Kyberuhkien analysoinnin uhkiksi tutkimuksessa [5] nimetään teollisuusvakoilun ja valtiollisten toimijoiden kyvykkyys, terrorismi, ohjelmistokehityksen pysyminen uhkien mukana, sisäpiiri- ja henkilöstöriskit ja avainhenkilöstöön sekä keskittyneisiin palveluihin kohdistuvat kyberuhkat. Toimintaverkoston analysoinnissa uhkina nähdään muun muassa resurssikapeikot laajojen häiriöiden tilanteissa sekä osaamisen katoamisen ulkoistetuissa palveluissa tai taloudellisissa saneerauksissa. Toimintaverkoston analysointia haittaa myös yrityksien huono näkymä verkostoon ja sen riippuvuussuhteisiin.

Tutkimuksessa [5] huomattiin, että riskitarkastelua ja varautumissuunnittelua ollaan liittämässä liiketoimintayksiköiden vastuulle, mikä parantaa toiminnan ja siihen liittyvien uhkatekijöiden yhteyttä. Harjoittelutoimintaa erityisesti Huoltovarmuuskeskuksen johdolla pidetään tutkimukseen haastateltujen yrityksien näkökulmasta

tärkeänä ja hyvänä toiminnan kehittämismahdollisuutena.

## 2.3 Kyberturvan nykytilan tutkimusta Euroopasta

ENISAn *Threat Landscape* [38, 39] on yksi Euroopan kyberturvallisuuden nykytilaa kartoittavista vuosittaisista raporteista. Se ei juuri ota kantaa erityisesti valmistavaan teollisuuteen tai kyberturvallisuuden tulevaisuuteen, mutta muutoin käsittelee kyllä aihetta laajasti. Vuonna 2017 ilmestyneessä raportissa [38] on listaus *Top Threats 2016*, jossa luetellaan 15 kyberuhkaa ja uhkatrendiä vuodelta 2016 ja verrataan niitä edellisen vuoden trendeihin. Viisi ensimmäistä uhkaa ovat haittaohjelmat, web-pohjaiset hyökkäykset, web-applikaatio hyökkäykset, palvelunesto (DoS) ja bottiverkot. Kaikkien näiden trendi on myös kasvava.

Näistä ENISAn raportissaan [38] listaamista uhkista useimmat pätevät luultavasti myös suomalaiseen valmistavaan teollisuuteen. Erityisesti valmistavaa teollisuutta koskevaksi uhkaksi ENISA mainitsee vuonna 2016 julkaistussa raportissaan [39] kybervakoilun, joka käytännössä on usein tietojenkalastelua. Kybervakoilun ENISA on sijoittanut listallaan kahtena vuotena peräkkäin sijalle 15, mutta vaihtanut sen trendin uudemmassa raportissa nousevasta laskevaksi [39, 38].

Europol sen sijaan ennustaa vuoden 2016 IOCTA-raportissaan (Internet Organised Crime Threat Assessment) [41], että valmistava teollisuus tulee näkemään entistä enemmän omien tuotteidensa, esimerkiksi älykkäiden laitteiden ja robottien, tietoturva-aukkojen hyväksikäyttöä. Esimerkkinä Europol antaa autovalmistajat ja heidän tuotteissaan käyttämänsä tekniikan. Raportti alleviivaa lakien ja asetuksien tärkeyttä, sillä ne vaikuttavat lopulta suuresti siihen, kuka on vastuussa. Lisäksi Europol korostaa eri toimijoiden yhteistyön merkitystä kyberturvallisuuden takaamiseksi Euroopassa. Näitä kahta näkökulmaa lukuun ottamatta raportti ei juurikaan kosketa erityisesti suomalaisen valmistavan teollisuuden kyberturvallisuuden tulevaisuudennäkymiä.

Yksittäisiä valmistavan teollisuuden kyberturvallisuutta koskevia tutkimuksia on tehty Euroopassa muutamia. Hyvä esimerkki tällaisesta on norjalainen tutkimus turvallisesta informaation jakamisesta teollisessa esineiden internetissä [56]. Tutkimuksessa tehtiin aiheesta kysely, joka kohdistettiin öljy- ja maakaasuyrityksien johtajille ja kyberturvallisuusvastaaville.

## 2.4 Kyberturvan tulevaisuuden tutkimusta maailmalta

Yksi viime aikoina julkaistuista kyberturvallisuuden tulevaisuutta käsittelevistä kansainvälisistä julkaisuista on Davenportin ja Amjadin artikkeli *The future of cybersecurity* [57]. Siinä he ennustavat kyberturva-ammattilaisia työssään auttavien analytiikan sekä automatiikan olevan kyberturvallisuuden seuraavat nousevat trendit.

Samassa artikkelissa [57] kirjoittajat nostavat riskiksi myös IoT:n ja siihen liittyvät uhkat lähitulevaisuudessa, kun miljoonat laitteet liitetään verkkoon. Myös Gartner ennustaa, että IoT:n yleistyessä kyberturvallisuuden on muutettava nykyistä, lähinnä ennaltaehkäisyyn keskittyvää, lähestymistapaansa ja tasapainotettava se reaaliaikaisuuden sekä automatisoidun monitoroinnin kanssa. [58].

Edellisten lisäksi Davenportin ja Amjadin artikkelissa [57] nostetaan esille kyberturvaosaajien puute. Artikkelin mukaan jo aiemmin mainittujen analytiikan ja automatiikan lisääminen auttaa myös tähän ongelmaan. Automaattisten kyberturvaohjelmistojen odotetaan myös parantuvan tulevaisuudessa, jolloin niistä on myös enemmän hyötyä organisaatioiden kyberturvallisuuden parantamisessa. Gartner [59] kuitenkin muistuttaa, että mitkään analytiikan tai automatiikan tarjoamat hyödyt eivät auta, jos perusasiat, kuten IoT-turvallisuuden kovennukset, eivät ole ensin kunnossa.

Yhdysvaltalainen *Verizon 2017 Data Breach Investigations Report* [6] nostaa erityisesti valmistavaa teollisuutta koskevaksi kyberturvallisuusuhkaksi kybervakoilun. Se kuvataan ulkopuolisena uhkana, joka on soluttautunut uhrin verkkoon etsimään sensitiivistä sisäistä dataa sekä liikesalaisuuksia [7]. Verizonen mukaan kybervakoilun takana ovat usein valtiolliset toimijat tai kilpailijat. Vakoiluhyökkäyksen suosituin tekniikka on tietojenkalastelu (phishing), mutta tarkoitukseen käytetään myös esimerkiksi takaovia uhrin verkkoon. [6].

Eräs tunnettu kyberturvallisuuden tulevaisuutta käsittelevä raportti on McAfee Labsin *Threats Predictions* [60]. Iso teema, joka nostetaan esille vuoden 2017 raportissa ja koskee myös ainakin osaa suomalaisen valmistavan teollisuuden yrityksistä, on pilviturvallisuus. Pilvipalvelujen yleistyminen ja kehitys tuo valmistavalle teollisuudelle paitsi uusia mahdollisuuksia niin myös uhkia. Raportissa ennakoidaan, että luottamus pilveen tulee kasvamaan, mikä lisää sinne tallennettavan sensitiivisen tiedon määrää. Tämä taas lisää pilven kiinnostavuutta hyökkäyskohteena. Yleisesti yrityksien ennakoidaan kuitenkin pitävän tärkeimmät tietonsa edelleen omissa luotetuissa verkoissaan ja datakeskuksissaan. Lisäksi ennakoidaan konflikteja turvallisuuden ja

nopeus-, kustannus- ja tehokkuusvaatimusten välille.

McAfee Labs [60] arvioi, että vanhentuneet autentikointijärjestelmät tuottavat jatkossakin haasteita pilviturvallisuudessa, mikä johtaa heidän mukaansa siihen, että tulemme näkemään paljon identiteettivarkauksia sekä brute-force hyökkäyksiä ylläpitäjätunnuksia vastaan. Pilvihyökkäyksien ennakoidaan jopa hyppivän eri organisaatioiden välillä, jos nämä käyttävät samaa pilvipalvelua. Pilviturvallisuus haastaa myös lakeja ja säädöksiä, joiden McAfee Labs ennustaa jäävän teknologioiden kehityksestä pahasti jälkeen.

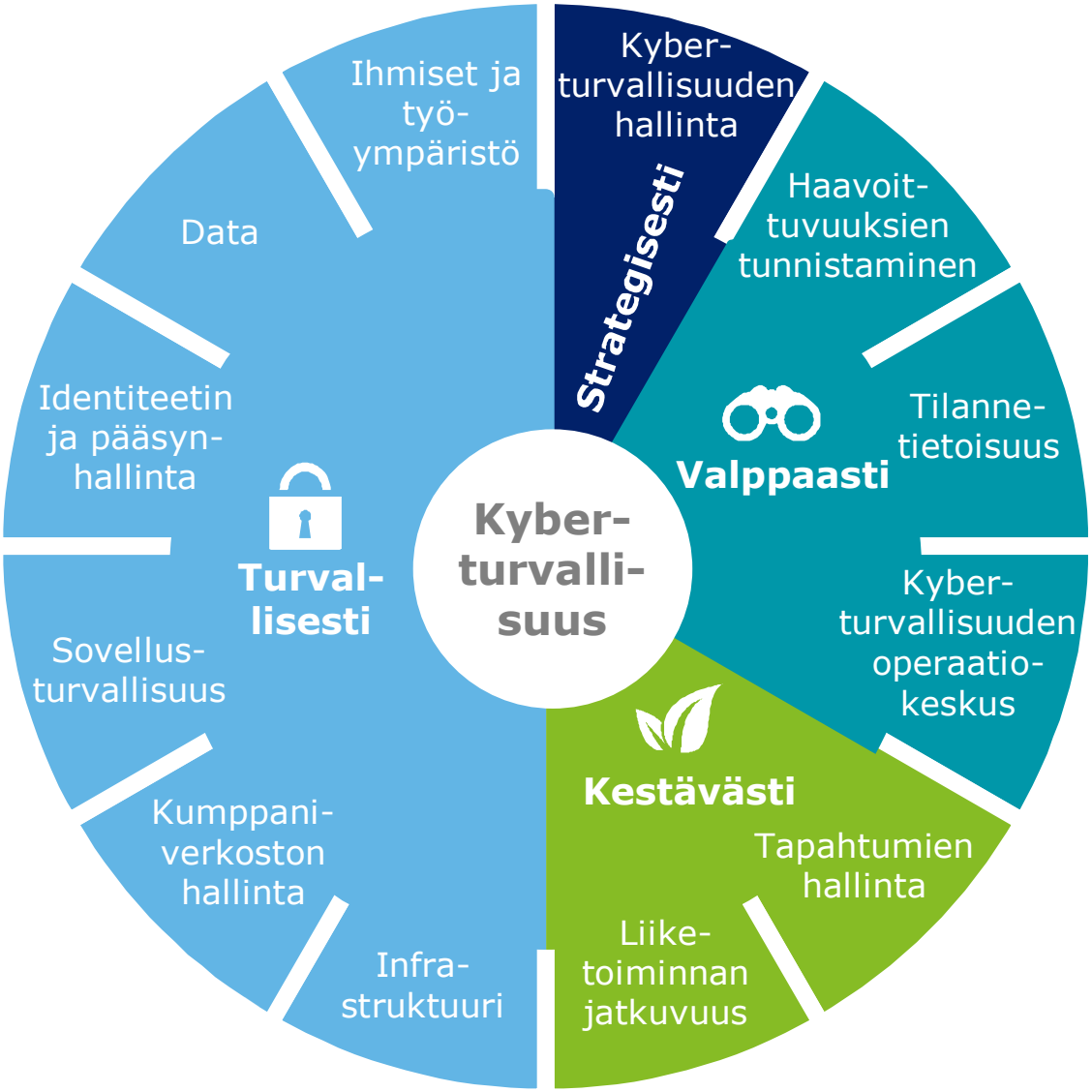
Edellä mainittujen lisäksi raportti [60] esittää pilviturvallisuuden lähitulevaisuuden haasteiksi ja hyökkäyksen kohteiksi aukot palvelukerrosten kattavuudessa sekä epäjohdonmukaisuudet asetuksissa ja kontrolleissa. Myös IoT-laitteita tullaan käyttämään apuna hyökkäyksissä. Näkyvyys ja kontrollointi pilvessä ovat lähitulevaisuudessa edelleen haasteita liiketoiminnalle, kun taas hyökkääjät tulevat käyttämään pilveä kasvattaakseen hyökkäyksiensä mittakaavaa, nopeutta ja anonymiteettiä. Lunnaita vaativat palvelunestohyökkäykset pilvipohjaisia organisaatioita kohtaan yleistyvät. McAfee Labs arvioi, että lukuun ottamatta käyttäjän autentikoinnin heikkouksia menestyksekkäitä julkiseen pilveen tallennetun datan vuotoja ei tulla juuri näkemään, mutta niiden vaikuttavuus kasvaa.

Onneksi lisääntyvien pilviturvallisuuden haasteiden ohella myös puolustuksen keinot kehittyvät. McAfee Labs ennakoi raportissaan [60], että salasanat tullaan lähitulevaisuudessa korvaamaan turvallisemmilla autentikointimenetelmillä. Muun muassa seuraavat teknologiat tulevat yleistymään ja helpottamaan pilven turvallisuutta: biometriikka, monitasoinen autentikointi ja käyttäytymisanalytiikka. Lisäksi liiketoimintatason näkyvyys ja kontrolli auttavat hallinnoimaan datan siirtoa pilveen silloin, kun käyttäjät käyttävät omia ratkaisujaan ja laitteitaan yrityksen hyväksymien sijasta. McAfee myös ennakoi, että pilvityöskentelyn kompleksisuutta ja volyymeja voidaan tulevaisuudessa hallita nykyistä paremmin.

Kuten Davenport ja Amjad omassa artikkelissaan [57] myös McAfee Labs [60] ennakoi, että turvallisuusautomaatio helpottaa jatkossa turvallisuusosaajien pulaa monella kyberturvallisuuden osa-alueella. Pilvien tietoturvaratkaisut alkavat myös käyttää koneoppimista, jota hyödynnetään proaktiivisessa tai jopa reaaliaikaisessa hyökkäyksien tunnistamisessa ja pysäyttämisessä.

## 2.5 Kirjallisuuskatsauksen yhteenveto

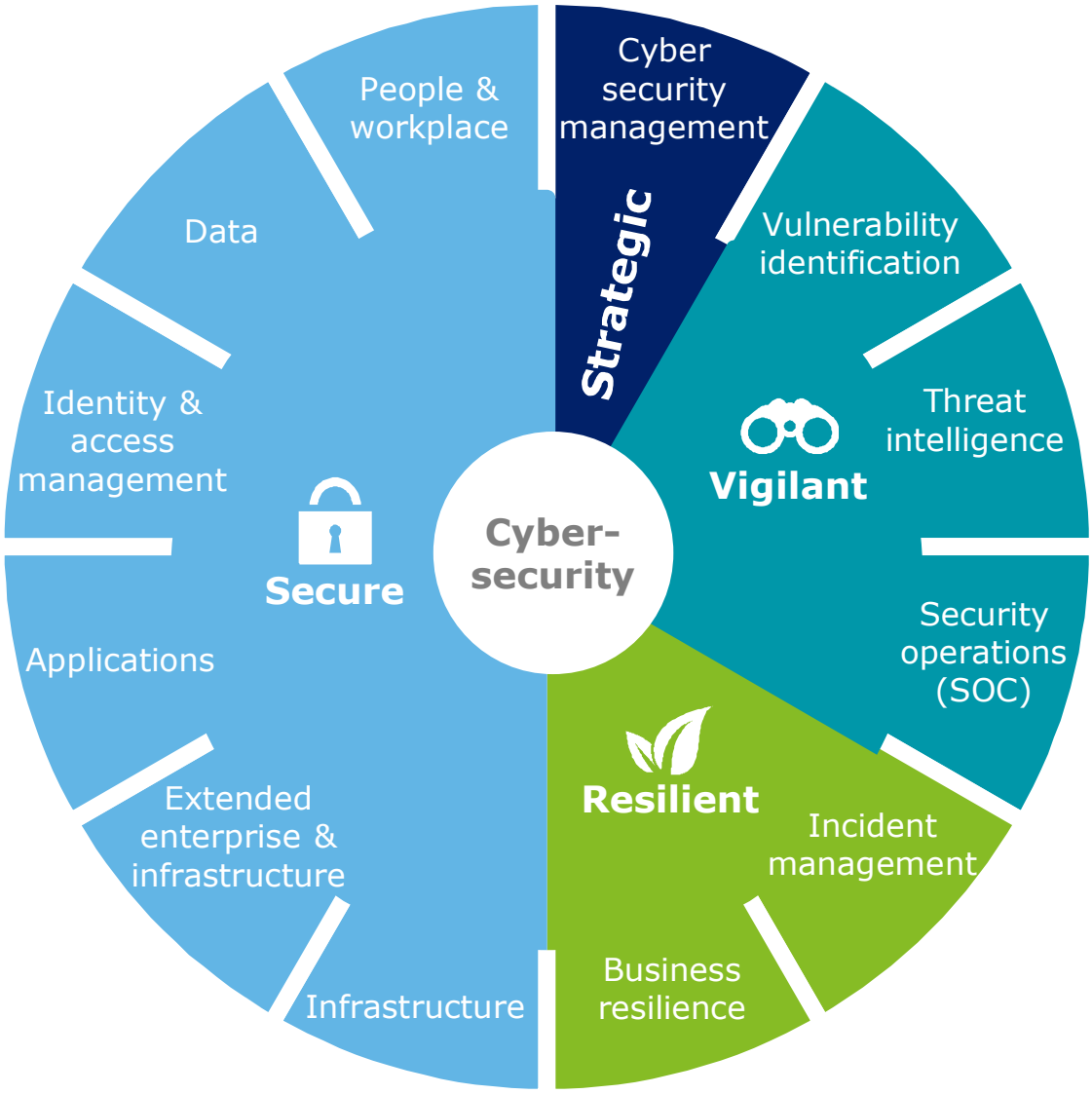
Kirjallisuuskatsauksen yhteenveto jäsenneltiin käyttäen apuna Deloitten kyberturvallisuuden viitekehystä (*Cyber Security Framework*) [61, 62, 63]. Yleensä viitekehystä käytetään englanniksi, mutta tämä tutkimuksen osana sen kompaktista muodosta laadittiin myös suomenkielinen versio, joka on alla olevassa kuvassa 2.1.




***Kuva 2.1*** *Deloitten kyberturvallisuuden viitekehys, kompakti muoto. Mukaillen [1].*

Alkuperäinen englanninkielinen versio on esitettynä seuraavalla sivulla kuvassa 2.2. Kuvan 2.1 suomennokset eivät kaikki ole suoria suomennoksia alkuperäisestä kuvan

2.2 versiosta vaan pikemminkin itse asiaa eli viitekehyksen eri osa-alueiden ja ala-osa-alueiden tarkoitusta ja tehtäviä kuvaavia.




***Kuva 2.2*** *Deloitte Cyber Security Framework, compact format [1].*

Kirjallisuuskatsauksen perusteella saatiin joukko erilaisia kyberturvallisuusaiheita pohjaksi valmistelu-työpajalle ja ensimmäiselle delfoi-kierrokselle. Seuraavaan taulukkoon 2.1 on koottu kirjallisuudesta kyberturvallisuusaiheita, jotka mahdollisesti vaikuttavat suomalaisen valmistavan teollisuuden tulevaisuudennäkymiin 4-5 vuoden päähän.

***Taulukko 2.1*** *Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuuteen vaikuttavia asioita kirjallisuudesta.*

| STRATEGISESTI (STRATEGIC / GOVERNANCE) | TURVALLISESTI (SECURE) |
|---|---|
| Esineiden internet eli IoT | Teollisuusautomaation (ICS) turvallisuus |
| Digitalisaatio ja "industry 4.0" | Saatavuuden varmistaminen |
| Käytettävyys vs. tietoturva | Identiteettien ja pääsynhallinta |
| Vaatimusten, lakien ja asetuksien täyttäminen ja muutokset | Vanhat teollisuusautomaatiojärjestelmät ja IT-ympäristöt |
| Eri maiden erilaiset lait | Pilviturvallisuus |
| Työntekijöiden kyberturvatietoisuus | Yksityisyydensuoja / tietosuoja |
| Tietoturvaosaajien puute | Mobiililaitteet |
| Nuorten työntekijöiden sitouttaminen kyberturvalliseen kulttuuriin | Vastuiden määritys toimittajien ja muiden kumppanien kanssa |
| Kasvavat suorituskyky ja reaaliaikavaatimukset | Kiristys ja terrorismi |
| Kyberturvallisuusresurssien puute ja kohdistaminen | IoT ransomwaren suosion kasvu |
| | Robotiikan turvallisuus |
| | Muutoksien ja päivityksien hallinta |
| | Kasvien datamäärien hallinta |
| **VALPPAASTI (VIGILANT)** | **KESTÄVÄSTI (RESILIENT)** |
| Nollapäivähaavoittuvuuksien hyödyntäminen | Kybervakoilu, myös valtiollisten toimijoiden tekemä |
| Edistyneet/kohdistetut kyberhyökkäykset (eli APT, Advanced Persistent Threats) | Kyberhyökkäyksiin varautuminen ja niistä toipuminen |
| Sisäpiiriuhkat | |
| Automaation ja analytiikan lisääntyvä käyttö kyberturvallisuuden parantamisessa | |
| Huijaukset | |
| Hyökkääjien ja hyökkäyksien tunnistaminen | |
| Tietoturvan monitorointijärjestelmät | |

Taulukon 2.1 kyberturvallisuusaiheet on jaoteltu Deloitten kyberturvallisuuden viitekehyksen (kuva 2.1) mukaisesti Strategisesti (*Strategic*), Turvallisesti (*Secure*), Valppaasti (*Vigilant*) ja Kestävästi (*Resilient*) -osa-alueiden alle. Strategisesti-osa-alueesta on lähteestä riippuen käytössä myös nimitys Hallinto (*Governance*).

### 2.5.1 Strategisesti

Useimmat taulukossa 2.1 olevista kyberturvallisuusaiheista liittyvät vahvasti kahteen Strategisesti-osa-alueen alle kuuluvaan kohtaan eli IoT:hen ja digitalisaatioon - jotka nekin liittyvät toki vahvasti toisiinsa. IoT:n turvallisuudesta ja riskeistä kirjoitetaan paljon mediassa, ja se mainitaan usein monissa valmistavan teollisuuden kyberturvallisuutta tutkivissa julkaisuissa sekä Euroopassa että muualla. Suuressa maailmanlaajuisessa tutkimuksessa 61 % tietohallintojohtajista sanoo yrityksiensä IoT-investointien kasvavan seuraavan kahden vuoden aikana [16].

Teollisuuden kyberturvallisuudesta puhuttaessa toinen usein käytetty termi on kyberfyysiset tuotantojärjestelmät (cyber-physical production systems). Näistä järjestelmistä taas koostuvat älykkäät tehtaat (smart factories), joiden tuotantojärjestelmät siis organisoivat ja optimoivat itse itsensä resurssien kulutuksen ja saatavuuden mukaisesti, jopa ylittäen yrityksen rajat. [64]. Älykkäät tehtaat ovat osa niin kutsuttua Industry 4.0:aa eli teollistumisen neljättä vallankumousta, jossa uudet teknologiat kuten pilvilaskenta, lisätty todellisuus, IoT, koneoppinen ja automaatio muuttavat teollisuutta. [65].

Kuten muuallakin maailmassa [42, 66], myös Suomessa valmistavan teollisuuden digitalisaation, industry 4.0:n ja IoT:n kyberturvallisuus vaikuttaa tällä hetkellä olevan suurissa määrin vielä strategisella tasolla. Toisin sanoen nyt tehdään päätökset siitä, kuinka turvallinen Suomen valmistavan teollisuuden tulevaisuuden kybertoimintaympäristö vuonna 2021 on. IoT:n tulevaisuudesta on ennakoitu, että keskiverto IoT-laite on murrettu oltuaan verkossa, lähteestä riippuen, vain kuusi tai kaksi minuuttia [67, 11] ja että vuoteen 2020 mennessä verkossa on kiinni yli 24 miljardia IoT-laitetta [68]. Toisaalta taas hieman uudempi ennuste sanoo, että kytkettyjä IoT-laitteita, sensoreita ja toimilaitteita on yli 46 miljardia ennen vuotta 2021 [69]. Usein erot ennusteissa näyttävät selittyvän sillä, lasketaanko älypuhelimia IoT-laitteiksi vai ei.

IoT:n turvallisuus on laaja käsite, johon liittyy monia erilaisia toimintoja ja toimijoita, alustoja, riskejä ja mahdollisuuksia. Usein teollisuuden IoT:stä puhuttaessa puhutaan IIoT:sta, joka on lyhenne englannin sanoista Industrial Internet of Things. [64]. Hyökkääjän näkökulmasta IIoT ei juuri eroa muista hyökkäyskohteista, mutta onnistuneen hyökkäyksen vaikuttavuus on usein paljon suurempi kuin esimerkiksi perinteisemmissä kuluttaja-orientoituneiden IoT-laitteisiin kohdistuneissa hyökkäyksissä. [56]. Tämä ei ainakaan vähennä IIoT:n suosiota hyökkäyskohteena tule-

vaisuudessa.

Muun muassa IoT-laitteita sisältävissä kyberfyysisistä tuotantojärjestelmissä on erilaisia abstraktiokerroksia, joista jokainen voi toimia alustana erilaisille hyökkäyksille. Tällaisia ovat esimerkiksi elektroniikka ja siihen kohdistuvat fyysiset hyökkäykset tai esimerkiksi viruksilla murrettavissa olevat ohjelmistot. Oman abstraktiokerroksensa muodostavat myös viestintäprotokollat, joihin voidaan kohdistaa protokollahyökkäys kuten välistäveto- ja palvelunestohyökkäys (MItM ja DoS). Lisäksi yhden tärkeän abstraktiokerroksen luovat tehtaiden omat sekä kolmansien osapuolien työntekijät. Heihin hyökkääjät voivat kohdistaa esimerkiksi erilaisia social engineering -hyökkäyksiä, kuten tietojenkalastelua. Jokainen uusi työntekijä, yhteistyökumppani tai IoT-ympäristöön liitetty uusi IoT-laite luo uuden hyökkäysalustan kyberfyysistä tuotantojärjestelmää vastaan. [64, 70, 71, 58, 61, 72].

Taulukon 2.1 kohta *vaatimusten, lakien ja asetusten täyttäminen ja muutokset* liittyy läheisesti sekä kyberfyysisiin tuotantojärjestelmiin että tietosuojaan ja datan keräämiseen [60, 64, 72]. Usein kyberfyysinen tuotantojärjestelmä esimerkiksi antaa mahdollisuuden BigData-teknologioiden käyttöön datan analysoinnissa, joka luo tarpeen ajatella tarkemmin muun muassa työntekijöiden yksityisyyden sekä asiakkaiden datan suojaukseen liittyviä vaatimuksia. [64].

Muun muassa Gartner [58] ja AT&T [66] ennakoivat seuraavan viiden vuoden aikana aktiivisuuden lisääntyvän uusien turvallisuusvaatimusten, standardointien ja parhaiden käytäntöjen kehittämisessä luonnostaan avoimiin IoT-ympäristöihin. Näin ollen myös suomalaisen valmistavan teollisuuden yrityksien on järkevää varautua tulevaisuudessa täyttämään yhä tiukempia IoT-ympäristöjen turvallisuusvaatimuksia.

Kyberturvallisuuden lait ja vaatimukset ovat myös erilaisia eri maissa [60], mikä vaikuttaa erityisesti globaalien yritysten toimintaan. Toisaalta kirjallisuus näkee tiukkojen ohjeiden ja teknisten standardien kehittämisen tärkeänä kyberturvallisuuden tukemisessa [72], mutta toisaalta taas yrityksien näkökulmasta esimerkiksi tietosuojasäädöksien kääntöpuolena on niiden rajoittavuus sisäpiiriuhkan valvonnassa. [12].

Gartner ennakoi myös, että tulevien vuosien aikana ei tulla näkemään sekä liiketoiminnalle, turvallisuudelle että käyttäjille ideaalia kaiken kattavaa ja yhtenäistä IoT-turvajärjestelmää, vaan todellisuus on lähinnä erillään olevia ympäristöjä ja niihin yksitellen liitettyjä turvajärjestelmiä [58]. Lisäksi tutkimusten [64, 60] mukaan tämänhetkiset IoT-järjestelmien turvallisuusratkaisut eivät vielä skaalaudu tarpeeksi,

jotta ne voisivat turvata laajat, hyvin erilaisia laitteita sekä kyberfyysisiä järjestelmiä sisältävät verkot samalla, kun täyttävät kasvavat reaaliaikaisuus- ja resurssivaatimukset.

Työntekijöiden tietoturvatietoisuus nyt ja tulevaisuudessa on asia, joka selvästi puhuttaa kirjallisuudessa (Suomea koskien esimerkiksi [35, 36, 5]). Tärkeäksi koetaan muun muassa henkilökunnan koulutuksen social engineering -hyökkäyksiä vastaan [72]. Lisäksi kirjallisuus nostaa esille tietoturvaosaajien puutteen isona tulevaisuuden ongelmana [57, 73] ja Viestintävirasto näkee sen kasvavan ongelmaksi Suomessa jo vuonna 2017 [36]. *Global Information Security Workforce Study 2017* [73] ennakoi, että vuonna 2022 maailmassa on jo 1,8 miljoonan kyberturvallisuustyöntekijän vaje.

Myös nuorten työntekijöiden sitouttaminen kyberturvalliseen kulttuuriin on puhuttanut viime vuosina. Aihe on tärkeä erityisesti kyberturvallisuuden tulevaisuutta ajatellen, sillä kyberturvallisuusosaajien puutteen alkaessa näkyä milleniaalien on paikattava tätä vajetta. Vanhempien sukupolvien kyberturvallisuusosaajien eläköityessä milleniaalien on otettava yhä suurempaa vastuuta yrityksien kyberturvallisuudesta, mutta esimerkiksi Iso-Britannia on jo nyt kohdannut haasteita milleniaalien rekrytoimisessa alalle. [73, 74, 75, 76, 77].

Tutkimukset [76, 77] osoittavat, että milleniaaleilla on erilaiset toimintatavat, arvot ja tarpeet kuin edellisillä sukupolvilla. Näin ollen yrityksien on tehtävä asioita erilailla kuin ennen sitouttaakseen milleniaalit paikkamaan kyberturvallisuusalan osaajavajetta. Milleniaalit esimerkiksi arvostavat organisaation koulutusohjelmia edellisiä sukupolvia enemmän. Milleniaalit myös vaihtavat työpaikkaa edellisiä sukupolvia helpommin, ja usein vaihto tehdään parempien etuuksien perässä. [76]. Lisäksi milleniaalien työskentelytavat eroavat aiemmista sukupolvista. He esimerkiksi kiertävät tietoturvakontrollit edellisiä sukupolvia todennäköisemmin [74].

Halukkuutta tähän kontrollien kiertoon on toki myös muissa sukupolvissa [74]. Kiertämisen estämiseksi on tärkeää, että työntekijät ymmärtävät kontrollien merkityksen ja että kontrollien käytettävyys on hyvä. Käytettävyyttä onkin joskus pidetty turvallisuuden vastakohtana - usein historiallisista syistä, sillä vanhat tietoturvaratkaisut saattoivat haitata huomattavasti jonkin järjestelmän käytettävyyttä. Tietoturvallisuustoimijat eivät myöskään ole aina olleet kovin kiinnostuneita käytettävyydestä.

Nykyään kuitenkin käytettävyyden katsotaan ennemminkin tukevan tietoturvalli-

suutta. Yleinen turvallisuus paranee, jos turvallisuustoiminnot ovat käytettäviä, sillä silloin ihmiset käyttävät niitä. [78]. Hyvä esimerkki ovat salaustyökalut, jotka yrityksen on tuotava työntekijöilleen vaivattomasti käytettäviksi tai muuten niitä ei käytetä [66]. Tutkimuksia tietoturvan ja käytettävyyden suhteesta on tehty myös esimerkiksi työntekijöiden käyttäytymistä tutkimalla [79].

### 2.5.2 Turvallisesti

Perinteiset IT-järjestelmät ja kyberfyysiset tuotantojärjestelmät eroavat toisistaan monessa kohtaa. Yksi suuri ero on järjestelmien turvallisuuden tavoitteissa. Perinteisen IT-järjestelmän tärkeimmät tavoitteet ovat eheys ja luottamuksellisuus, ja siksi sen kyberturvallisuus usein onkin kompromissi saatavuuden ja turvallisuuden välillä. Tällöin kyberhyökkäyksen sattuessa voidaan hyökkäyksen eteneminen estää sammuttamalla IT-järjestelmä hetkellisesti tai eristämällä se verkosta.

Samaa ei sen sijaan voi tehdä kyberfyysiselle tuotantojärjestelmälle, jolta vaaditaan erityisesti saatavuutta ja jonka seisokit ovat erittäin kalliita. Näin ollen kyberfyysisissä tuotantojärjestelmissä suurinta vahinkoa aiheuttavat viivästymiseen johtavat hyökkäykset. Nämä viivytykset saavat aikaan tehokkuuden ja tulojen menetyksiä. Tästä syystä esimerkiksi suojautuminen palvelunestohyökkäyksiä vastaan on valmistavalle teollisuudelle tärkeää. [64].

Lee, Bagheri ja Jin kuvaavat tutkimuskirjeessään *Introduction to cyber manufacturing* [72] valmistavan teollisuuden tärkeimmiksi kyberhaasteiksi standardien puutteen, BigDatan käsittelyn ja kyberturvallisuuden. Näiden haasteiden ratkaiseminen on pakollista, jotta esimerkiksi esineiden internetistä ja kyberfyysisistä tuotantojärjestelmistä on mahdollista saada irti kaikki niiden tarjoama hyöty. Heidän mukaansa kyberturvallisuus vaatii yhdistäviä äly-ohjattuja lähestymistapoja eikä ainoastaan työkaluriippuvuutta.

IoT:n ja kyberfyysisten tuotantojärjestelmien turvallisuuden yhteydessä kirjallisuudessa törmää usein ICS:n (Industrial Control System) kuten SCADAn (Supervisory Control and Data Acquisition) turvallisuuteen. Nämä teollisuuden ohjausjärjestelmät ovat viime vuosina muuttuneet suljetuista ja yksilöllisistä ympäristöistä avoimiin arkkitehtuureihin ja standardoituihin teknologioihin [40].

ICS-ympäristöjen avautuminen ja kytkeytyminen IT-järjestelmiin on avannut paljon uusia mahdollisuuksia hyökkääjille ja siten heikentänyt myös Suomen valmistavan

teollisuuden kyberturvallisuutta. ICS:n erityisenä haasteena ja kriittisenä tekijänä on tarve hallita liiketoimintaoperaatioita vuorokauden ympäri vuoden jokaisena päivänä. Tämä ICS:n pitäisi tehdä ilman suunnittelemattomia tuotantoseisokkeja. [70]. ICS-hyökkäyksissä on jo vuoden 2016 aikana havaittu suurta kasvua: esimerkiksi IBM:n mukaan 110 prosenttia vuoteen 2015 verrattuna [80].

Tutkimusten mukaan [70, 58, 61, 56, 60, 81, 59] yleinen IoT-ympäristöjen turvallisuuden ongelma on, että IoT-ekosysteemiin liitetään vanhoja, jo käytössä olevia sensoreita. Tämä perustellaan taloudellisilla syillä, sillä vanhojen sensoreiden kytkeminen on yleensä halvempaa kuin uusien ostaminen. Nämä sensorit eivät kuitenkaan ole suunniteltu liitettäväksi isoihin avoimiin verkkoihin, jolloin niiden turvallisuus ei ole riittävällä tasolla. Niin ikään vanhat IT-turvallisuuskontrollit tai -perustuotteet kuten identiteetin ja pääsynhallinnan työkalut eivät ole riittäviä IoT:n turvallisuustarpeille.

Melkein poikkeuksetta IoT-ekosysteemiin kuuluu paljon erilaisia sekä ylä- että alavirtaan toimitusketjussa sijoittuvia organisaatioita ja sidosryhmiä. Yleensä kaikki osat tässä ketjussa tuottavat ja käsittelevät dataa, ja koko toimitusketjun hallinta ja turvaaminen saattaa olla haastavaa. Tällöin on tärkeää huolellisesti määrittää datan omistajuus sekä elinkaari. [61]. Lisäksi kirjallisuudessa mainitaan tulevaisuuden haasteeksi kolmansien osapuolien kyberturvallisuuden takaamisen muutoinkin kuin vain IoT-ekosysteemeissä - esimerkiksi tulevaisuudessa erilaisia palveluja tullaan ulkoistamaan entistä enemmän, jolloin kyberturvallisuusvastuiden määritys on erittäin tärkeää. [14].

Yhdeksi selväksi tulevaisuuden kyberturvallisuusongelmaksi tutkimuksissa nimetään kasvavien datamäärien hallinta. Mobiililaitteiden, BigDatan, IoT:n ja vastaavien teknologioiden kehityksen ja suosion myötä data tulee liikkumaan yhä enemmän ja sen määrä maailmassa tulee kasvamaan. Näin ollen myös sen hallitseminen turvallisesti on tulevaisuudessa yhä hankalampaa. Jokaisen yrityksen onkin tärkeää huolellisesti määrittää ja dokumentoida yhdessä toimittajien ja kumppanien kanssa kuka on vastuussa mistäkin. Tällä on tarkoitus varmistaa, että esimerkiksi IoT-ekosysteemissä jokainen tietää tarkasti oman vastuualueensa rajat ja ymmärtää alueeseensa liittyvät kyberriskit. Lisäksi yritysten on tarpeellista miettiä paitsi datan omistajuuskysymyksiä niin myös sitä, mitä tietoa ylipäätään on kannattava kerätä ja säilyttää. [70, 66].

Näin ollen yrityksien on nykyään yhä haastavampaa tietää kuka, miten ja mis-

sä heidän dataansa käsittelee. Tulevaisuudessa tämä korostaa yhä enemmän identiteettien ja pääsynhallinnan tärkeyttä samoin kuin tiedon luokittelun. [66]. Tutkimusten [56, 42, 81, 66] mukaan myös informaation turvallinen jakaminen IIoT-ekosysteemeissä ja erityisesti IIoT-tapauksissa on tulevaisuuden haaste, joka täytyy ratkaista. Informaation turvallisessa jakamisessa IIoT-ekosysteemeissä haasteellisia ovat skaalautuvat ratkaisut identiteettien hallintaan ja valtuuksiin, sisältäen avaintenhallintaprotokollat, salausprotokollien päivitykset ja digitaaliset sertifikaatit. Muun muassa tässä monet IoT-protokollat ovat osoittautuneet virheellisiksi.

Yleinen, useammassa raportissa [5, 60, 81, 66] esille tullut ja myös suomalaisia yrityksiä koskeva, kyberturvallisuuden huolenaihe on pilvipalvelujen turvallisuus. Yritykset siirtävät pilveen yhä enemmän dataa sekä palveluja. Näin ollen pilvipalveluissa sijaitsee paljon dataa, joka on yrityksen liiketoiminnalle kriittistä: esimerkiksi luottamuksellisia talous-, innovaatio-, asiakkuus-, yritysoperaatio- tai henkilöstötietoja. Pilvipalvelut eivät kuitenkaan välttämättä ole turvattomampia kuin muut IT-palvelut. Oleellista on, että palvelun hallinnoijat tarkistavat konfiguroinnin oikeellisuuden. Myös datan suojaaminen ja pääsynhallinta on tärkeää. Pilvipalveluihin suositellaankin käytettäväksi kaksiosaista todentamismenetelmää.

Yksi pilvipalvelujen ongelma on työntekijöiden henkilökohtaisessa käytössä olevat pilvipalvelut. Näihin, usein yrityksien omia pilvipalveluja turvattomimpiin, ympäristöihin työntekijät saattavat varastoida myös työhönsä liittyvää sensitiivistä tietoa. [81]. Pahimmillaan työntekijät käyttävät näitä henkilökohtaisia pilvipalvelujaan turvattomasti ja samalla käsittelevät siellä huolimattomasti yrityksen sensitiivistä dataa.

Omien pilvipalvelujen ohella työntekijät käsittelevät yrityksiensä tietoa yhä enemmän omissa mobiililaitteissaan. Mobiililaitteiden kyberturvallisuus onkin useissa vuoden 2017 ennusteissa [60, 36, 81, 66] esiintyvä teema. Kirjallisuudessa ennakoidaan kiristyshaittaohjelmien kasvattavan suosiotaan mobiilissa samoin kuin esimerkiksi sensitiivisten tietojen varastaminen mobiililaitteiden huijaussovelluksilla. Kirjallisuuskatsauksessa ei kuitenkaan selvinnyt, että onko mobiililaitteiden kyberturvallisuus enää vuonna 2021 erityisen tärkeää, vai ehditäänkö siihen jo muutamassa vuodessa tottua ja varautua.

Pilvi- ja mobiiliturvallisuuden lisäksi myös robotiikan turvallisuus on esillä kirjallisuudessa. Tutkimukset [41, 5, 82] esimerkiksi ennustavat, että hyökkääjät tulevat lähitulevaisuudessa käyttämään robottien tietoturva-aukkoja hyväkseen. Myös

IoT ransomware -kiristyshyökkäyksien suosion ja volyymien kasvu aiheuttaa vakavia ongelmia tulevaisuudessa [43, 36, 60, 12]. Kiristyksen ohella IoT:n tulevaisuuden haasteisiin kuuluu sen haavoittuvuuksien mahdollinen käyttö terrorismin välineenä [60]. Lisäksi IoT:n yleistyminen lähitulevaisuudessa tuo paljon muutoksia tietosuojaasioihin [83, 60, 84, 64, 61] vielä Euroopan GDPR:n voimaan astumisen jälkeenkin. Kirjallisuudessa on saatavilla aiheesta paljon pohdintaa sekä ohjeita (esimerkiksi [85]).

### 2.5.3 Valppaasti

On arveltu, että *sisäpiiriuhka* [56, 5, 12] on yksi suurimmista tulevaisuuden IIoT-uhkatyypeistä. Paitsi omat työntekijät niin myös muut sidosryhmät saattavat olla valtuutettuja pääsemään käsiksi ja/tai kontrolloimaan verkon sensoreita. Tällöin uusien toiminnallisuuksien tai laitteiden lisääminen verkkoon tai niiden poistaminen esimerkiksi toimittajan puolesta voivat olla vakavia kyberturvallisuusuhkia.

Valppaasti-osa-alue tulee kehittymään tulevaisuudessa, kun muun muassa *automatiikan ja analytiikan käytön kyberturvallisuuden parantamisessa* ennustetaan lisääntyvän ja olevan yksi seuraavista kyberturvallisuuden trendeistä [57, 81, 66]. Lisäksi myös erilaisten *huijauksien* suosion ennakoidaan jatkuvan lähitulevaisuudessa [36, 35]. Tutkimusten [5, 71, 58, 86, 81] mukaan hyökkäyksien, huijauksien ja hyökkääjien seuraavien liikkeiden ennakoiminen ja tunnistaminen yhä nopeammin on tulevaisuudessa entistä tärkeämpää. Tällöin kyberturvallisuus ei olisi enää vain reaktiivista vaan muun muassa parempien monitorointijärjestelmien ansiosta myös proaktiivisuus, tai jopa reaaliaikaisuus, olisi mahdollista.

Erityinen tulevaisuuden haaste kyberturvallisuuden monitorointijärjestelmille, sekä muutenkin organisaatioiden kyberturvallisuudelle, ennakoidaan olevan *edistyneet (tai kohdistetut) kyberhyökkäykset (APT, Advanced Persistent Threats)*. Ne ovat vaarallisia, sillä niiden vaikutukset kohteeseensa ovat merkittävämmät kuin yleisillä hyökkäyksillä. Tutkimukset osoittavat, että kohdistetut kyberhyökkäykset ovat yleistyneet viimevuosina. APT:n lisäksi *nollapäivähaavoittuvuudet* ennakoidaan ongelmiksi myös tulevaisuudessa. [36, 35, 72]. Tästä huolimatta yrityksien ei tarvitse torjua kaikkein vaikeimmin tunnistettavissa olevia kyberhyökkäyksiä ollakseen paremmassa turvassa. Jo pelkästään *tunnistamalla yleisimmät ja tunnetut hyökkäykset* nykyistä nopeammin, käyttäen apuna esimerkiksi automatiikkaa, monien yrityksien kyberturvallisuus paranisi nykyisestään jo huomattavasti. [81].

### 2.5.4 Kestävästi

Taulukon 2.1 kohta *kybervakoilu* nousee esille sekä kyberturvallisuusraporteissa että mediassa tasaisin väliajoin (esimerkiksi YLEn [87] ja the Washington Timesin [88] uutiset aiheesta). Vakoiluhyökkäyksiä on monenlaisia, useimmiten esimerkiksi kilpailijoiden yrityksiä saada haltuunsa organisaation liikesalaisuuksia ja IP-dataa (intellectual property). Tällainen kiinnostava data voi koskea esimerkiksi tuotantoprosesseja, patentteja, designia, tuotekehitysdataa tai reseptejä. Sensitiiviseen dataan käsiksi pääsemiseen hyökkääjä voi käyttää esimerkiksi haavoittuvia IoT-laitteita. [42, 6, 6].

Kybervakoiluriskejä punnittaessa on muistettava, että nykypäivän globaalissa markkinassa kansainväliset kilpailijat eivät välttämättä pelaa samoilla säännöillä kuin suomalaiset yritykset. Tämän tyyppiset organisaatiot voivat nähdä kybervakoilun yksinkertaisesti tavallisena liiketoiminnan kuluna. Joissain maissa kybervakoilua rahoittavat valtiolliset toimijat. [89, 6]. Kaspersky Lab uskoo kybervakoilun leviävän yhä enemmän mobiililaitteisiin jo vuonna 2017 [44].

Edellisten lisäksi *kyberhyökkäyksiin varautuminen ja niistä toipuminen* on asia, johon yritysten on alettava kiinnittää yhä enemmän huomiota tulevina vuosina. Kaikilla yrityksillä täytyy olla ajantasaiset suunnitelmat kyberhyökkäyksestä toipumiseen. Torjuntasuunnitelmat kyberhyökkäyksien varalle täytyy myös pitää ajan tasalla, jotta proaktiivinen kyberturvallisuus on mahdollista. [81, 66].

# 3. TUTKIMUSMENETELMÄ DELFOI

Koska delfoi on laajasti tunnettu ja käytetty tulevaisuudentutkimuksen menetelmä, on sillä ja sen eri variaatioilla laaja vertailupohja historiasta. Vuosikymmenien aikana sen ominaisuuksia on sekä arvosteltu että ylistetty. [32, 28, 29, 31]. Osmo Kuusi kuvaa artikkelissaan [29] tyypillisen delfoi-tekniikkaa käyttävän tutkimuksen vaiheet seuraavasti:

1. tutkimusongelman rajaus ja tutkimuksen tavoitteiden määrittely
2. suunnittelevan tutkijaryhmän kokoaminen tutkimuksen toteuttamista varten
3. varsinaisen asiantuntijapaneelin kokoaminen ja valinta
4. kyselylomakkeen rakentaminen, testaaminen ja korjaus ensimmäistä kyselykierrosta varten
5. ensimmäinen kyselykierros joko kirjallisena (tai atk-avusteisena) tai suullisena haastattelukyselynä
6. ensimmäisen kyselykierroksen vastausten analyysi
7. toisen kierroksen kyselylomakkeen rakentaminen ja mahdollinen testaus
8. toisen kyselykierroksen toteuttaminen ja vastausten arviointi
9. raportointi tutkimuksen tuloksista.

Tässä tutkimuksessa haastattelukierroksia tehtiin yllä olevan esimerkin mukaisesti kaksi, joka on tyypillinen kierrosmäärä nykyajan delfoi-tutkimuksissa. Delfoin ensimmäisen iteraatiokierroksen tarkoituksena on etsiä olennaisia kysymyksiä ja motivoida asiantuntijapaneelia jatkotyöskentelyyn. Tämä toimii siten jälkimmäisen kierroksen pohjana, jolloin saadaan asiantuntijoilta palaute ensimmäisen kierroksen aiheista. Palautteisuus onkin delfoille perinteisesti tunnusomaista ja erottaa sen muun

muassa gallupeista. Palaute annetaan ensimmäisellä kierroksella tunnistetuista väittämistä ja jokainen asiantuntijapanelisti perustelee vastauksia erilaisin argumentein eli näkökohdin. [28].

Asiantuntijapanelistien valinta on delfoi-prosessin kriittisimpiä vaiheita. Delfoi-tutkimuksessa henkilö katsotaan asiantuntijaksi silloin, kun hän pystyy arvioimaan ja ennustamaan kyseistä asiaa tai ilmiötä paremmin kuin ei-asiantuntija. [29]. Jokainen tämän tutkimuksen panelisti on kokenut valmistavan teollisuuden kyberturvallisuuden asiantuntija: he työskentelevät valmistavan teollisuuden yrityksissä ja käsittelevät kyberturvallisuutta päivittäisessä työssään.

Kuusi mainitsee artikkelissaan [29] myös, että delfoi-paneelin asiantuntijat kannattaa valita siten, että yhdessä he edustavat monipuolisesti tutkittavan aihepiirin kehittäjäyhteisöä eli toimijoita, joiden työhön aihe olennaisesti kuuluu. Kyberturvallisuuden parissa voi työskennellä monenlaisella koulutus- ja asiantuntijuustaustalla. Näin ollen tämän tutkimuksen paneeliin valittiin erilaisia taustoja omaavia asiantuntijoita: osan tausta oli esimerkiksi enemmän tietotekniikassa ja kyberturvallisuuden teknisellä puolella, kun taas osan erityisosaaminen enemmän kyberturvallisuuden hallinnollisella puolella. Kenellekään asiantuntijapanelisteista kyberturvallisuuden kokonaisuus ei kuitenkaan ollut vieras.

Delfoi-menetelmässä tutkimuksen vetäjän tehtäviin kuuluu kierroksien välissä koota tulokset ja esittää ne paneelille seuraavan kierroksen pohjaksi [29]. Lisäksi delfoi-tutkimuksen vetäjän on tärkeää suojella panelistien anonymiteetti sovitulla tavalla [32].

## 3.1 Miksi delfoi

Yksi tärkeimmistä syistä siihen, että tämän tutkimuksen menetelmäksi valikoitu juuri delfoi, on asiantuntijapaneelin keskustelijoiden tunnistamattomuus. Yrityksien kyberturvallisuudesta puhuttaessa keskustelijoiden tunnistamattomuuden tärkeys korostuu, sillä keskusteltavat asiat saattavat sisältää sensitiivistä tietoa paitsi yrityksen liiketoiminnasta myös yksittäisen asiantuntijan työuran näkökulmasta. Delfoita käytettäessä asiantuntijat uskaltavat siis helpommin sanoa suoraan, mitä ajattelevat, eivätkä esimerkiksi seuraa mielipiteissään yrityshierarkiassa arvostetumman tittelin omaavaa keskustelijaa. Toisin sanoen, kun keskustelijoiden statuksia ei tiedetä, niin jokaisen mielipide painaa yhtä paljon. Anonyymisyys myös eliminoi dominoivien

henkilöiden vaikutuksen sekä ryhmäpaineen päätöksentekotilanteessa. [32, 31].

Tämän tunnistamattomuuden varjopuolena saattaa tietenkin olla, että keskustelijat eivät välttämättä mieti omia vastauksiaan riittävän syvällisesti, koska nimettöminä he eivät voi menettää kasvojaan vaikka vastaisivat pinnallisesti. Kyseinen heikkous on kuitenkin kierrettävissä haastattelemalla asiantuntijoita online-lomakkeiden sijaan kasvokkain. Silloin asiantuntijalla on varattuna haastatteluun kuluva aika asian pohtimiseen. Lisäksi, kun aikaa on tarpeeksi, keskustelijan voi olla myös helpompi päästä yleistä tasoa syvemmälle ja hyödyntää asiantuntijuuttaan vastauksissaan. Online-kysely saatetaan täyttää nopeasti ja huolimattomasti, kun taas järkevästi strukturoidussa haastattelussa asiantuntijan saattaa olla helpompi tuoda ajatuksiaan enemmän esille.

Lisäksi online-kyselylomakkeisiin verrattuna kasvokkain tehtyjen haastattelujen etuna on mahdollisuus huomata ja korjata mahdollisia väärinymmärryksiä sekä tarvittaessa tarkentaa kysymyksiä. Väärinymmärryksien mahdollisuutta pienentää myös delfoin toinen kierros, jonka aikana asiantuntijat voivat tutustua muiden argumentteihin sekä korjata omia kannanottojaan [32]. Tätä vastoin online-kyselyjen ongelmana saattaa olla, että ohjeistus kyselyn täyttämiseen ei ole tarpeeksi selvää, ja vastaukset ovat tämän takia virheellisiä ja jopa täysin hyödyttömiä. Lisäksi avoimia kohtia sisältävien online-kyselyjen yksi huono puoli on niiden laadun riippuvuus vastaajan kirjoitustaidosta. Myös tämän ongelman kasvotusten tehty haastattelu kiertää.

Online-vastauksilla on toki hyvätkin puolensa verrattuna kasvokkain tehtyihin haastatteluihin. Online-kyselyillä vastaajia voidaan helpommin tavoittaa suurempi joukko. Tämä on hyödyllistä, jos määrällisen tutkimuksen ominaisuudet ovat tutkimuksen päämäärien näkökulmasta tavoittelemisen arvoisia. Online-kyselyssä haastateltu asiantuntija on myös mahdollista anonymisoida täysin jopa tutkimuksen tekijältä. Tämän tutkimuksen delfoi-kierrokset ovat kuitenkin määrällisten online-kyselyiden sijasta haastatteluja kasvokkain tai puhelimitse, sillä tämä tukee parhaiten tutkimuksen tavoitteiden saavuttamista.

Tunnistamattomuudelle ja koko delfoi-menetelmän toimimiselle on kriittistä, että asiantuntijat on valittu tarkasti ja heidän asiantuntemuksensa on tarkoituksenmukaista tutkimuksen päämääriä ajatellen. Monialaista näkemystä haluttaessa asiantuntijapanelistit voidaan valita aivan eri aloilta, mutta myös saman alan edustajien keskuudessa saattaa olla näkemyseroja, jolloin delfoi antaa jokaiselle mahdollisuuden

esittää oma näkemyksensä.

Kääntöpuolena oikeiden henkilöiden huolellinen valinta voi myös viedä kauan aikaa ja heidän tavoittamisensa saattaa olla haastavaa. Yksi riski delfoi-tutkimuksen onnistumiselle onkin tutkimuksen tavoitteita ajatellen juuri oikeiden henkilöiden tunnistaminen ja tavoittaminen. Lisäksi delfoita on joskus arvosteltu sen mahdollisesti kasvavien rahallisten ja ajallisten kustannuksien takia.

Rahallisten ja ajallisten kustannuksien pitäminen alhaisina oli kuitenkin melko helppoa tämän kokoisessa tutkimuksessa. Toki jokaisella panelistilla meni tähän tutkimukseen aikaa vähintään pari tuntia, mutta osallistumisen vapaaehtoisuuden nimissä niitäkään tunteja on hieman haastavaa arvioida esimerkiksi rahallisesti. Tutkimuksen tekijälle tutkimuksesta ei juuri syntynyt kuin hieman kustannuksia pääkaupunkiseudun sisällä haastatteluihin liikkumisesta. Suurimman osan kustannuksista kantoikin tämän tutkimuksen teettäjä Deloitte, joka maksoi tutkimuksen tekijälle palkkaa myös tutkimuksen tekemiseen käytetystä ajasta. Lisäksi Deloittelle syntyi kustannuksia, kun sen asiantuntijat käyttivät aikaansa muun muassa valmistelutyöpajaan osallistumiseen ja muuten tutkimuksen tekijän tukemiseen. Kaikki tutkimukseen osallistuneet toki saivat, ainakin toivottavasti, tutkimuksesta kustannuksilleen myös jotain vastinetta.

Delfoin hyvänä puolena pidetään yleisesti sen joustavuutta ja sopivuutta erikokoisiin tutkimuksiin. Sitä on käytetty sekä maailmanlaajuisissa tuhansien henkilöiden vastaajajoukot vaatineissa tutkimuksissa että esimerkiksi kuuden hengen asiantuntijaryhmän pienessä selvityksessä. Asiantuntijapaneelin koosta huolimatta kriittistä tutkimuksen onnistumisen näkökulmasta on asiantuntijoiden valinta sekä sitouttaminen. [29].

Asiantuntijoiden nopeaa sitouttamista tukee delfoin iteratiivinen luonne: kun toisen kierroksen alussa panelisteille näytetään muiden panelistien nimet, saattavat he kyseisellä kierroksella olla sitoutuneempia esimerkiksi vastaamaan huolellisemmin esitettyihin kysymyksiin. Asiantuntijapaneelin nimien paljastaminen panelisteille on muun muassa disaggretative-delfoissa ja Rauchin päätöksenteko-delfoissa käytetty asiantuntijoiden motivointikeino. Delfoi on siis matkan varrella kehittyvä menetelmä, jonka luotettavuus kasvaa kierros kierrokselta. [32].

Delfoin iteratiivisuudella on myös varjopuolensa, joka johtuu delfoin yhteistä ymmärrystä hakevasta luonteesta. Joihinkin tutkimuksiin delfoi ei siis sovi, koska tätä

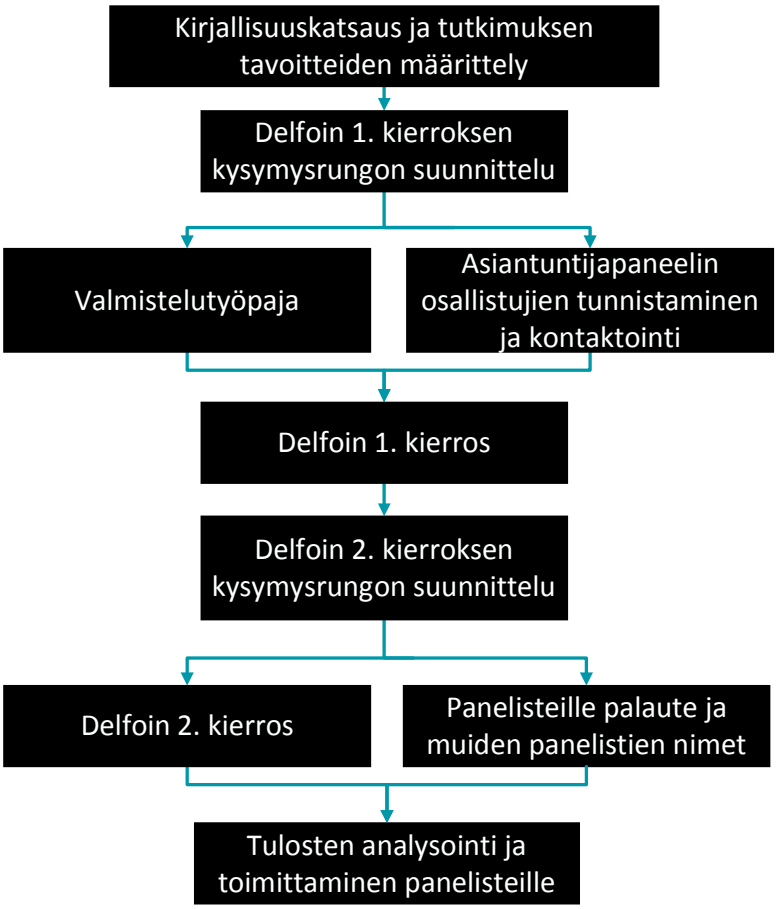
yhteistä mielipidettä hakiessa se saattaa jättää heikot trendit sekä innovatiivisimmat ratkaisut huomioimatta. Toisin sanoen delfoi siis kierros kierrokselta rajaa pois ääripäitä jättäen lopuksi jäljelle keskimäärin tärkeimmäksi koetun vastauksen esitettyyn kiistakysymykseen. [29]. Tässä tutkimuksessa tähän kiinnitettiin erityistä huomiota, jotta myös mahdolliset heikot tulevaisuuden trendit tunnistettaisiin.

## 3.2 Delfoi-tutkimuksen toteutus

Tämä tutkimus jaettiin kolmeen vaiheeseen. Ensimmäinen vaihe koostui delfoi-tutkimuksen ensimmäisen kierroksen huolellisesta valmistelusta: kirjallisuuskatsauksesta, valmistelutyöpajasta sekä asiantuntijapaneelin jäsenten valinnasta ja kontaktoinnista. Huolellinen valmistelu on tärkeää, jotta vältetään delfoin tunnettuja heikkouksia kuten vääränlaisen asiantuntijapaneelin kokoamista, heikosti suunniteltuja haastattelukysymyksiä tai perusteettomia ja liian ohjailevia hypoteeseja.

Tutkimuksen seuraava vaihe oli delfoin ensimmäinen kierros, jonka tarkoituksena oli tutustuttaa asiantuntijapaneelin jäsenet aiheeseen ja tutkimukseen sekä viedä läpi valmisteluvaiheessa luotujen hypoteesien ensimmäinen iteraatiokierros. Delfoin ensimmäisen kierroksen jälkeen jäljelle jäivät suosituimmat näkemykset suomalaisen valmistavan teollisuuden kyberturvallisuuden tulevaisuudesta. Nämä näkemykset koottiin yhteen ja niiden perusteella valmisteltiin palaute seuraavaa iteraatiokierrosta varten.

Ensimmäisen kierroksen perusteella suunniteltiin huolellisesti delfoin toinen kierros. Sen päätteeksi saatiin kuva suomalaisen valmistavan teollisuuden kyberturvallisuuden tulevaisuudennäkymistä sekä siitä, mitkä asiat tätä lähitulevaisuutta tarkasteltaessa ovat kaikkein tärkeimpiä. Tämä delfoi-tutkimusprosessi ja siihen liittyvät vaiheet on kuvattu kuvassa 3.1.




***Kuva 3.1*** *Delfoi-tutkimusprosessi*

On huomattava, että kaikki kuvan vaiheet eivät välttämättä olleet täysin perättäisiä, vaan esimerkiksi asiantuntijapaneelin mahdollisia jäseniä tunnistettiin koko valmisteluvaiheen ajan ja myös valmistelutyöpajassa. Kuvassa näkyy siis vasta lopullinen asiantuntijapaneelin jäsenten kontaktointi, mitkä tehtiin samoihin aikoihin valmistelutyöpajan kanssa ja saatettiin päätökseen osittain jo ensimmäisten haastattelujen alettua.

### 3.2.1 Valmistelu

Ensimmäisessä vaiheessa luotiin alustavat hypoteesit sekä delfoi-menetelmän ensimmäisen kierroksen kysymysrunko. Tämä kysymysrunko suunniteltiin ja valmisteltiin alan kirjallisuuskatsauksen (luku 2) pohjalta. Lisäksi kysymysrungon hahmottelemiseen käytettiin apuna paljon suomalaisen valmistavan teollisuuden parissa työs-

kennelleiden kyberturvallisuusasiantuntijoiden näkemyksiä. Näille henkilöille järjestettiin työpaja, jossa muun muassa hiottiin kysymysrunkoa ja kartoitettiin siihen sopivia aiheita.

Samaan aikaan kun tässä valmisteluvaiheessa delfoi-haastatteluille luotiin pohja, niin myös alan yrityksistä tunnistettiin ja kontaktoitiin sopivat henkilöt delfoissa käytettävää asiantuntijapaneelia varten. Tätä varten tutkimuksesta ja sen tavoitteista valmisteltiin lyhyt esittely, jossa kerrottiin, mitä asiantuntijapanelisteilta odotetaan ja mitä he itse voivat tutkimukseen osallistumisesta saada. Asiantuntijat kontaktoitiin ensin sähköpostikutsulla ja sen jälkeen muutaman päivän päästä puhelimella, jos he eivät olleet reagoineet sähköpostiin.

Tutkimukselle ei siis asetettu tarkkoja hypoteeseja ennalta, vaan delfoi-tutkimuksen tuloksia peilattiin kirjallisuuskatsaukseen ja delfoin ensimmäisen kierroksen alustaviin tuloksiin. Delfoin ensimmäistä kierrosta varten työpajassa ja kirjallisuuskatsauksessa hypoteeseja siis kerättiin laajasti, jotta delfoin kierrokset eivät olleet jo valmiiksi liian ohjailevia, mutta toisaalta eivät myöskään täysin perusteettomia.

Valmistelutyöpaja toteutettiin puolen tunnin sessiona, johon osallistui 14 suomalaisen valmistavan teollisuuden parissa työskentelevää kyberturvallisuuden asiantuntijaa Deloitten Cyber Risk -tiimistä. Yli puolet asiantuntijoista oli työskennellyt kyberturvallisuuden parissa yli viisi vuotta ja heistä suurin osa yli kymmenen vuotta. Tarkempi lista osallistuneista asiantuntijoista on liitteessä 1. Työpaja pidettiin syksyllä 2016, loka-marraskuun vaihteessa.

Työpajassa testattiin ja hiottiin delfoin ensimmäisen kierroksen kysymykset. Lisäksi tunnistettiin potentiaalisia asiantuntijapanelisteja ja tarkennettiin tutkimuksen tavoitteita. Työpaja pidettiin osittain englanniksi, sillä yksi osallistujista ei puhunut suomea.

Asiantuntipaneeliin asiantuntijat valittiin heidän asemansa perusteella suomalaisista valmistavan teollisuuden yrityksistä. Tarkoituksena oli koota paneeliin asiantuntijoita erilaisilla taustoilla sekä katsontakannoilla. Panelistien taustat ja työtehtävät osoittautuivatkin sopivan vaihteleviksi. Osalla oli enemmän esimerkiksi hallinnollisen puolen taustaa ja osalla taas takanaan pitkä ura tietotekniikan parissa. Asiantuntijapanelistit olivat turvallisuus-, tietohallinto-, kyberturvallisuus- tai tietoturvajohtajia. Asiantuntijapaneelin jäsenet on listattu liitteeseen 3.

Alun perin tarkoituksena oli saada paneeliin kymmenen asiantuntijaa, mutta koska yksi joutui perumaan viime hetkellä, oli paneelin lopullinen koko yhdeksän henkeä. Asiantuntijapanelisteista seitsemällä oli yli viiden vuoden kokemus kyberturvallisuuden parista ja heistä neljällä yli kymmenen vuoden kokemus. Kahdella kokemus oli alle viisi vuotta juuri kyberturvallisuudesta, mutta heilläkin ennen kyberturvallisuuteen keskittymistä oli vuosien tai vuosikymmenien kokemus tietotekniikasta, jolloin tieto- ja kyberturvallisuus on ollut osana työtä.

### 3.2.2 Ensimmäinen delfoin-kierros ja alustavien tuloksien analyysi

Kun aiheet ja kysymysrunko (liite 2) delfoin ensimmäiselle kierrokselle oli valmisteluvaiheen aikana suunniteltu ja testattu, siirryttiin itse haastatteluihin. Haastatteluista neljä ensimmäistä pidettiin joulukuussa 2016 kasvotusten. Haastattelut jatkuivat alkuvuodesta 2017, jolloin niitä pidettiin neljä kasvotusten ja yksi puhelinneuvotteluna Skype for Business -ohjelmalla. Yhteensä ensimmäisen kierroksen haastatteluja pidettiin siis yhdeksän.

Haastattelujen perusteella valmistavan teollisuuden yritysten tilanne Suomessa vaikuttaa siltä, että niissä on tunnistettu kyberriskit esimerkiksi virallisella kyberturvallisuuden auditoinnilla tai riskikartoituksella. Näin ollen yritykset tuntuivat siis tietävän, kuinka niiden kyberturvallisuutta saataisiin parannettua. Useimmissa yrityksissä näitä asioita oli jo aloitettu toteuttaakin, ja vähintään suunnitelmia seuraavan viiden vuoden aikana tehtäviin parannuksiin oli laadittu.

Useassa ensimmäisen kierroksen haastattelussa tuli esille kyberturvallisuustoimijoiden verkostoitumisen merkitys. Asiantuntijat kokivat tiedon jakamisen tärkeäksi tulevaisuuden keinoksi pitää yllä suomalaisen valmistavan teollisuuden kyberturvallisuutta ja siten myös liiketoimintaa. Turvallisuustoimijoiden ja saman alan yrityksien verkostoitumisessa asiantuntijat korostivat erityisesti luottamusta ja vastavuoroisuutta. Keskusteluissa useampi panelisti mainitsi Viestintäviraston tärkeäksi viranomaiseksi, joka koordinoi ja mahdollistaa verkostoitumisen alalla.

Myös tutkimukset toteavat kyberturvallisuuden olevan joukkuepeliä [5, 90]. Esimerkiksi VVT:n tutkimus *Menestyvää liiketoimintaa suomalaisissa valmistavan teollisuuden yrityksissä 2020-luvulla* [23] sanoo yrityksien verkostoitumisesta ja tulevaisuuteen varautumisesta: "Valmistautuakseen muutokseen yrityksen on aktiivises-

ti seurattava vahvoja tai heikkoja signaaleja, jotka ennakoivat toimintaympäristön muutoksia. Signaalien tarkkailua ja tulkintaa helpottaa aktiivinen verkostoituminen teknologian ja liiketoiminnan asiantuntijoiden sekä muiden yritysten johdon kanssa." Yrityksillä on siis sitä paremmat edellytykset varautua kyberuhkiin, mitä enemmän eri toimijoiden välillä jaetaan tietoa kybertoimintaympäristöstä ja sen tapahtumista.

Myös Suomen kyberturvallisuusstrategia [2] tukee verkostoitumista. Sen mukaan kybertoimintaympäristön muutosnopeus ja kompleksisuus edellyttävät uudenlaista verkostomaista toimintamallia, joka perustuu vahvaan koordinaatioon ja yhteisiin pelisääntöihin. Tässä toiminnassa on kyettävä yhdistämään keskittämisen ja hajauttamisen edut, jotka ovat vahva koordinaatio ja asianomistajuudesta syntyvä reagointinopeus. Vastaavaa verkostoitumista edistetään myös muualla maailmalla, esimerkkinä Online Trust Alliance OTA, jonka tulevaisuuden visio on tuoda kehittäjät, kauppiaat ja päättäjät proaktiivisesti vastaamaan yhdessä IoT:n tulevaisuuden haasteisiin kehittämällä parhaita käytäntöjä, standardeja sekä benchmarktutkimusta [71].

Ensimmäisen kierroksen haastatteluissa ilmeni monia samoja asioita kuin valmisteluvaiheen kirjallisuuskatsauksessa ja työpajassa. Jonkin verran ilmeni myös uusia asioita. Liitteeseen 5 on koottu lista asioista, jotka panelistit mainitsivat haastatteluissa useampaan kertaan Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuuteen vaikuttavina asioina.

Yleisesti ensimmäisen kierroksen perusteella asiantuntijapanelistit tuntuvat suhtautuvan Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuuteen positiivisesti. He uskoivat, että viiden vuoden päästä kyberturvallisuus on yrityksissä yhä arkipäiväisempi asia, joka kuuluu kaikkeen toimintaan: se ei ole enää erillinen päälle liimattava "laastari" vaan pikemminkin osa prosesseja ja kaikkea toimintaa.

Panelisteilta tuli toiveita, että suomalaisen valmistavan teollisuus olisi ottanut viiden vuoden päästä pitkiä askelia eteenpäin kyberturvallisuudessaan. He perustelivat toivettaan, sillä koko yhteiskunnan ja myös valmistavan teollisuuden riippuvuus IT-järjestelmistä tulee yhä kasvamaan, hyökkäyksistä tulee yhä älykkäämpiä ja kyberrikollisuudesta yhä ammattimaisempaa. Asiantuntijat uskoivat, että eri yrityksissä tulee kuitenkin olemaan edelleen eroja, mutta isojen ja verkostoituneiden yrityksien asiat tulevat olemaan suhteellisen hyvin. Suomen hyvän koulutustason, tasapainoisen toimintaympäristön ja vakaiden maantieteellisten ja poliittisten olosuhteiden

nähtiin luovan hyvät edellytykset kyberturvalliselle toiminnalle.

Vaikka delfoi-menetelmällä on yleensä etsitty yhteisymmärrystä, nykyään menetelmää käytetään usein myös innovaatio- ja oppimisjärjestelmänä, jolloin arvoa annetaan myös eriäville mielipiteille [91, 31, 32]. Näin ollen tässäkään tutkimuksessa ei ensimmäisen kierroksen jälkeen ollut tarkoitus saada yhtä ainoaa oikeaa vastausta vaan tavoitteena oli myös innovoida ja oppia jakamalla tietoa osallistujien kesken. Innovointi tarkoitti tässä muun muassa erilaisia tulevaisuudennäkymiä, jotka voisivat olla mahdollisia suomalaisen valmistavan teollisuuden kyberturvallisuudelle. Haastattelutilanteet olivat kiireisille asiantuntijoille toki myös mahdollisuuksia pysähtyä hetkeksi miettimään yrityksensä ja teollisuudenalansa kyberturvallisuuden kokonaiskuvaa sekä tulevaisuutta.

Usein delfoin jatkokierroksilla syvennetään kysymyksenasettelua esitettyjen argumenttien perusteella. Niistä voidaan esimerkiksi luoda uusia tulevaisuuskysymyksiä entisten lisäksi, jolloin tutkimus laajenee, tai sitten tutkimusta fokusoidaan ja rajataan niin, että jatkokierroksille ”selviää” vain osa alkuperäistä kyselyä. [29]. Ensimmäisen kierroksen jälkeen tätä tutkimusta toisaalta rajattiin, kun huomattiin, mitkä kysymykset ovat tutkimuksen kannalta mielekkäitä. Toisaalta tutkimusta taas laajennettiin ensimmäiseltä kierrokselta nousseisiin mielenkiintoisiin aiheisiin, jotka esitellään tarkemmin seuraavassa luvussa 3.2.3 toisen delfoi-kierroksen yhteydessä.

### 3.2.3 Toinen delfoi-kierros ja alustavien tuloksien iterointi

Delfoin toinen iteratiivinen kierros suunniteltiin ensimmäiseltä kierrokselta saatujen alustavien tuloksien perusteella. Sitä varten ensimmäisellä kierroksella saadut tiedot oli analysoitava tarkasti ja niiden kommunikointi panelisteille mietittävä, jotta he pystyivät muuttamaan ja edelleen perustelemaan käsityksiään. Tässä on kyse delfoille ominaisesta palautteisuudesta.

Toisen kierroksen haastattelut sisälsivät siis ensimmäisen kierroksen alustavien tulosten esittelyä. Samalla kysyttiin esimerkiksi panelistien mielipidettä edellisen kierroksen perusteella muotoillusta kyberturvallisuuden määritelmästä. Sen lisäksi ensimmäiseltä kierrokselta oli kerätty suomalaisen valmistavan teollisuuden kyberturvallisuuden tilaa ja tulevaisuudennäkymiä kuvaavia väittämiä, joita panelistit pääsivät kommentoimaan tarkemmin toisella kierroksella - puolustamaan näkemystä tai esittämään vasta-argumentteja. Nämä väittämät oli jaoteltuna kolmeen kategoriaan:

miksi, mitä ja miten kyberturvallisuutta tehdään viiden vuoden päästä. Väittämät ovat liitteessä 4.

Lisäksi ensimmäiseltä kierrokselta nousi muutamia teemoja, joista jatkokysymysten esittäminen toisella kierroksella oli tarpeen väärien tulkintojen välttämiseksi. Jatkokysymyksiä esitettiin esimerkiksi kyberturvallisuusinvestointien mittaamisesta sekä yrityksen kyberturvallisuuskulttuurin kehittymisestä tulevaisuudessa. Toisella kierroksella paneelilta myös kysyttiin lisää teemoista, jotka jäivät ensimmäisellä kierroksella vähemmälle huomiolle, mutta jotka huomattiin mielenkiintoiseksi alustavien tuloksien analyysissä. Tällaisia teemoja olivat hieman panelistista riippuen esimerkiksi yrityksen kyberturvallisuuden tavoite sekä kipukohdat.

Toisen kierroksen aluksi, ennen itse haastatteluja, panelisteille lähetettiin sähköpostilla lyhyt tehtävä. Tehtävä koski ensimmäisen kierroksen haastattelujen perusteella koostettua listausta kyberturvallisuusaiheista (liitteessä 5). Tästä listasta jokaista panelistia pyydettiin valitsemaan ne, jotka hän näkee vuonna 2021 olevan suomalaisen valmistavan teollisuuden kyberturvallisuuden näkökulmasta viisi tärkeintä ja vastaavasti viisi vähiten tärkeintä. Vastaukselle ei tässä vaiheessa vaadittu perusteluja, vaan aiheeseen palattiin toisen kierroksen haastatteluissa. Näin ollen toisen kierroksen haastattelussa asiantuntijat pääsivät argumentoimaan mielipiteensä puolesta ja avaamaan ajatusketjuaan valintojensa takana. Lisäksi delfoin palautteisuutta hyödynnettiin, kun panelistit pääsivät jo tässä vaiheessa kuulemaan, mitä muut panelistit olivat vastanneet tehtävään etukäteen ja vertaamaan omia valintojaan muiden valintoihin.

Delfoin palautteisuus toimi myös toiseen suuntaan, kun asiantuntijat kommentoivat delfoi-tutkimuksen vetäjälle toisen kierroksen haastattelujen aikana, että listasta (liite 5) oli vaikea valita viisi vähiten tärkeintä. Viiden tärkeimmän valintaa pidettiin helpompana tehtävänä. Panelisteista useimmat kuitenkin lopulta valitsivat viisi vähiten tärkeitä mielessään se, että onko asia jo mahdollisesti paremmin hallittu vuonna 2021, jolloin siihen ei tarvitse juuri enää keskittää kyberturvallisuuden resursseja. Tämä lopulta muodostuikin "vähemmän tärkeän asian"määritelmäksi, sillä kuten panelistit sanoivat, mitään listan asioista ei voi kyberturvallisuustekemisessä täysin unohtaa, koska milloinkaan ei voi olla täysin varma, että mitään ei tapahdu.

Toisen kierroksen haastattelut pidettiin maaliskuussa 2017 kasvotusten lukuun ottamatta yhtä Skype for Business -puhelinhaastattelua. Toisen kierroksen kysymysrungot valmisteltiin ensimmäisen kierroksen tulosten perusteella helmikuun 2017

lopussa. Kaikilta kysyttävien asioiden lisäksi jokaiselle panelistille esitettiin myös muutamia panelistikohtaisia kysymyksiä, jotka tarvitsivat ensimmäisen kierroksen pohjalta vielä tarkennusta väärinkäsitysten ja virheiden eliminoimiseksi. Toisen kierroksen jälkeen tutkimuksen tulokset koottiin yhteen ja analysoitiin. Delfoin tulokset sekä niiden tulkinta ovat seuraavassa luvussa 4.

# 4. SUOMEN VALMISTAVAN TEOLLISUUDEN KYBERTURVALLISUUS VUONNA 2021

Tässä luvussa esitellään tarkemmin delfoin ensimmäisen ja toisen kierroksen jälkeen yhteen kootut ja analysoidut tutkimustulokset. Analyysissä, sekä osittain jo delfoi-kierroksien aikana, kartoitettiin käsitystä Suomen valmistavan teollisuuden kyberturvallisuudesta vuonna 2021. Tämä yleinen kuva muodostui siis alan asiantuntijoista koostuvan paneelin käsityksien pohjalta. Sanalla "paneeli" viitataan kaikkiin panelisteihin ja sitä käytetään, kun jostakin asiasta panelisteilla voidaan katsoa olleen yhteinen ymmärrys. Ensimmäiseltä delfoi-kierrokselta toiselle paneelin validoitaviksi nousseet asiat ja väittämät on tässä luvussa korostettu *kursiivilla*.

Jo ensimmäisen delfoi-haastattelukierroksen jälkeen asiantuntijapaneeli vaikutti suhtautuvan varsin positiivisesti suomalaisen valmistavan teollisuuden kyberturvallisuuden tulevaisuuteen. Tämä vaikutelma vahvistui myös toisella haastattelukierroksella. Toki panelistit näkivät, että asioiden hoitaminen kuntoon vaatii työtä ja isoja askelia täytyy ottaa eteenpäin, jotta asiat pysyvät hallinnassa, mutta kukaan ei esimerkiksi luonut skenaarioita, jossa Suomen valmistava teollisuus joutuisi suuriin ongelmiin tai jonkinlaiseen suureen kriisiin kyberturvallisuusongelmien takia.

Edistysaskelien ottamisen panelistit kokivat välttämättömänä, jotta Suomen valmistava teollisuus pystyy vastaamaan kyberuhkiin sen tulevaisuuden toimintaympäristössä, jossa riippuvuus tietoverkoista ja -järjestelmistä kasvaa entisestään samaan aikaan, kun hyökkäyksistä tulee yhä älykkäämpiä ja kyberrikollisuudesta yhä ammattimaisempaa. Paneeli kuitenkin uskoi, että Suomen hyvä koulutustaso, tasapainoinen toimintaympäristö ja vakaat maantieteelliset ja poliittiset olosuhteet luovat hyvät edellytykset kyberturvalliselle toiminnalle.

Vaikka tällä hetkellä yrityksessä kyberturvallisuusasiat näyttäisivät olevan ihan hyvin eikä mitään isoa olisi tapahtunut, ei kyberturvallisuustyötä voida lopettaa. Tämä tiivistyy hyvin ensimmäiseltä delfoi-kierrokselta nousseeseen väittämään, jonka

myös kaikki panelistit totesivat todeksi: *kyberturva on osa-alue, jossa jos liikut hitaasti, niin suhteellisesti liikut taaksepäin.* Esimerkiksi erään panelistin yrityksessä tämä oli huomattu myös käytännössä: "Kun saavutimme haluamamme kyberturvallisuustason, niin huomasimme tasolla pysymisen vaativan jatkuvaa ylläpitoa ja työtä."

Edellisen lisäksi muutama panelisti huomautti, että "rikolliset liikkuvat meitä nopeammin ja heillä on isommat investoinnit - vastapuolen ei myöskään tarvitse noudattaa lakeja toisin kuin meidän". Valmistavan teollisuuden uhkakartan paneeli sanoi muuttuvan myös erittäin nopeasti, mikä luonnollisesti sekin haastaa alan kyberturvallisuuden hallintaa. Nämä ovatkin syitä, miksi vuonna 2021 suomalaisen valmistavan teollisuuden täytyy edelleen panostaa kyberturvallisuuteensa.

Paneeli uskoi, että vuonna 2021 eri yrityksien kyberturvallisuudessa on varmasti edelleen eroja, mutta isojen ja verkostoituneiden yrityksien asiat tulevat olemaan suhteellisen hyvin. Verkostoitumista paneeli miettikin useampaan kertaan delfoi-haastattelukierroksien aikana ja kysymys siitä, *onko kilpailijoilla mahdollisuus verkostoitua kyberturvallisuusasioissa* nostettiin heidän pohdittavakseen ensimmäiseltä kierrokselta toiselle. Toisella kierroksella paneeli päätyi yleisesti siihen, että myös kilpailijoiden verkostoitumisen kyberturvallisuusasioissa pitäisi olla mahdollista.

Eräs asiantuntijoista kuvasi verkostoitumisen ja asioiden jakamisen olevan "keino selviytyä". Verkoistumisesta panelistit antoivat myös erilaisia esimerkkejä. He huomauttivat, että verkostoituminen ei ole keneltäkään pois eikä se riko millään tavalla kilpailulainsäädäntöä. Eräs panelisti näki kuitenkin, että ei-suorien kilpailijoiden verkostoituminen on yksinkertaisempaa kuin suorien.

Lisäksi eräs panelisteista mainitsi, että verkostoituminen on Suomessa ja länsimaissa helpompaa, sillä yrityksien ja yhteiskunnan kulttuurit esimerkiksi eettisen kilpailun keinoista ovat samanlaisia. Yksi asiantuntijoista huomautti, että tulevaisuudessa kyberturvallisuudesta voi myös tulla entistä tärkeämpi kilpailutekijä, jolla yrityksen on mahdollisuus erottautua. Hän kuitenkin jatkoi, että silti "edellä menevän kiinni saaminen" ei ole ihan realistista, mikä totta kai helpottaa verkostoitumista. Eräs panelisti summasi asian näin: "Täällä Suomessa on pakko tehdä yhteistyötä, sillä vastustajat ovat voimakkaita."

## 4.1 Mitä on kyberturvallisuus

Ensimmäisellä kierroksella paneelilta kysyttiin, kuinka he käsitteenä määrittelevät kyberturvallisuuden. Tähän tuli odotetusti vaihtelevia vastauksia ja näkökulmien painotuksia, mutta toiselle kierrokselle ne oli kuitenkin mahdollista tiivistää seuraavasti: "Kyberturvallisuus on lähinnä tietoturvan päälle laitettu uusi termi, joka laajentaa pelkän tietoturvan käsitettä koskemaan myös esimerkiksi IoT- ja tehdasympäristöjä." Toisella kierroksella paneeli hyväksyi tämän määritelmän.

Ensimmäisellä kierroksella useampi asiantuntija myös mainitsi kyberturvallisuuden koostuvan kolmesta osasta: prosessit, ihmiset ja teknologia. Jotkut panelisteista korostivat lisäksi sitä, kuinka nykyään ongelmat kyberturvallisuudessa heijastelevat myös fyysiseen maailmaan: esimerkiksi tehtaan suuriin koneisiin vaikuttamalla voidaan uhata ihmisten terveyttä tai henkeä. Muutama panelisti kuitenkin muistutti, että kyberturvallisuus on suurimmilta osin vanhaa tuttua tietoturvatekemistä, jota ei tule unohtaa uuden termin takia.

## 4.2 Mitä tavoitellaan

Asiantuntijapanelisteilta kysyttiin delfoin toisella kierroksella heidän yrityksensä kyberturvallisuuden tavoitteita. Heille annettiin valmiiksi ensimmäisen delfoi-kierroksen perusteella valitut vaihtoehdot, joista he valikoivat kaikki mielestään oman yrityksensä kyberturvallisuuden tavoitteita kuvaavat. Vaihtoehdot ja vastauksien jakaantuminen näkyvät kuvassa 4.1.


***Kuva 4.1*** *Tavoite kyberturvallisuudelle Suomen valmistavan teollisuuden yrityksissä.*

Kuten kuvasta 4.1 voi huomata, melkein jokainen panelisti valitsi annetuista tavoitevaihtoehdoista enemmän kuin yhden. *Vaatimuksien täyttämisen* panelistit valitsivat selvästi muita vaihtoehtoja useammin ja vain kaksi panelistia jätti sen valitsematta. Eräs asiantuntijoista sanoikin tämän olevan "ehdotonta". Seuraavaksi eniten panelistit valitsivat yrityksensä tavoitteiksi *parhaiden joukossa olemisen* sekä *kyberturvallisuudella kilpailuedun saamisen*. Kummatkin valittiin neljä kertaa ja vain yksi panelisti antoi yrityksensä tavoitteina näistä molemmat.

*Kilpailuetua kyberturvallisuudella* paneeli sanoi saavutettavan esimerkiksi turvallisen industry 4.0:lla sekä silloin, kun asiakkaat näkevät yrityksen luotettavampana kuin kilpailijansa. Paneeli katsoi hyvän laadun ja toimitusvarmuuden lisäävän yrityksen luotettavuutta, mutta niitä kumpaakin huono kyberturvallisuus saattaa heikentää. Eräs panelisteista mainitsi kuitenkin, että isossa, maailmanlaajuisessa yrityksessä textslkilpailuedun saavuttaminen kyberturvallisuudella on haastavaa.

Yksi, joka valitsi tavoitteeksi *parhaiden joukossa olemisen*, kertoi yrityksensä toimitusjohtajan ilmaiseen asian selvästi sanomalla pari kertaa, että "teettehän nyt tähänkin maailmanluokan ratkaisun". Muutama panelisteista kuitenkin näki, että yrityksen ei tarvitse olla paras: esimerkiksi erään panelistin mielestä *parhaiden joukossa oleminen* olisi "toki hienoa, mutta turhaa liiketoiminnan kannalta". *Parhaaksi pääsemisen* antoi yrityksensä kyberturvallisuuden tavoitteeksi vain yksi panelisti. Hän sanoi tämän kuuluvan yrityksen arvoihin, mutta toki matkalla parhaaksi "kaikki askeleet on kuitenkin tehtävä eikä siellä olla nopeasti".

Kenellekään panelisteista pelkkä *selviytyminen* ei ollut tavoite, mutta *pääsemisen muiden, esimerkiksi kilpailijoiden, tasolle* yrityksensä tavoitteeksi antoi kaksi panelistia. Toinen heistä kuvasi asian niin, että kyberturvallisuuden tason pitää olla sellainen, että "ei ole hitain saaliseläin liikkumassa". Yksi asiantuntijoista muistutti, että tämä tavoite voi vaihdella riippuen keneltä asiaa kysyy: ylin johto voi nähdä asian eri tavalla kuin esimerkiksi osakkeenomistajat tai kyberturvallisuuden asiantuntijat. Seuraavissa luvuissa käsitellään tarkemmin sitä, mitkä asiat panelistit näkivät tärkeäksi suomalaisen valmistavan teollisuuden kyberturvallisuuden näkökulmasta vuonna 2021. Eli toisin sanoen, mitkä asiat tulevat silloin vaikuttamaan eniten näihin kyberturvallisuuden tavoitteisiin pääsemiseen.

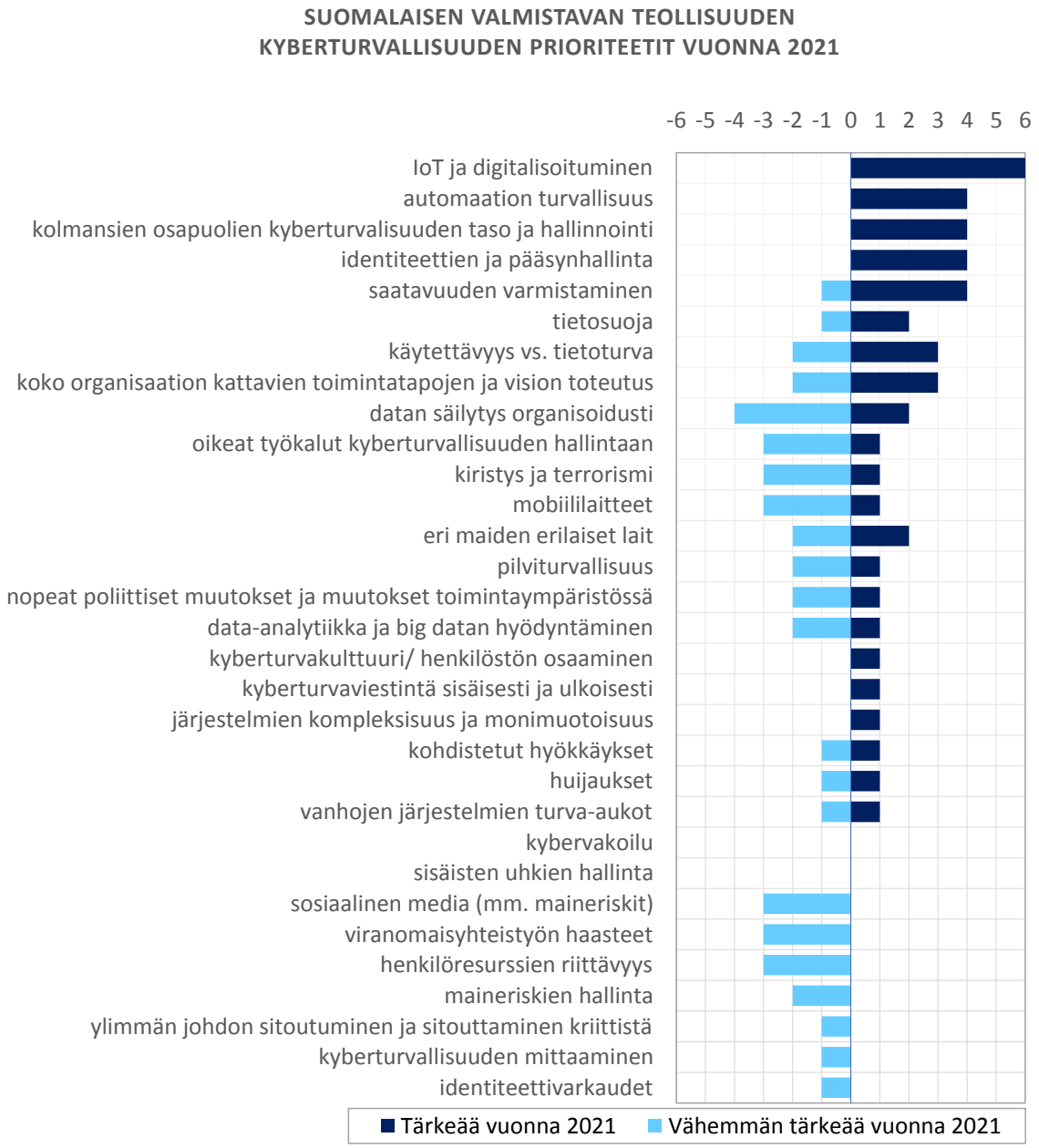
Paneelilta kysyttiin tavoitteiden lisäksi toisella delfoi-kierroksella, keneen he vertaavat kyberturvallisuuttaan - esimerkiksi ketkä ovat ne "parhaat", joiden joukossa halutaan olla. Osalle panelisteista tämä oli selvää ja he kertoivat vertaavansa esi-

merkiksi omaan toimialaansa tai muihin huoltovarmuusyrityksiin. Eräs panelisteista sanoi "kriittisen itsearvioinnin"olevan paras mittari, sillä suoraan muihin vertaaminen ei kerro kaikkea. Erään panelistien ehdottama "omaan menneisyyteen vertaaminen" onkin hyvä keino, jos esimerkiksi yrityksen kyberturvallisuustasoa arvioidaan säännöllisin väliajoin.

## 4.3 Mikä on tärkeää ja mikä vähemmän tärkeää vuonna 2021

Yrityksien kyberturvallisuus koostuu monista erilaisista asioista ja osista, joista kaikkiin on käytännössä mahdoton panostaa yhtä paljon. Näin ollen on tärkeää voida päättää, mihin käytössä olevat rajalliset resurssit kohdistetaan. Tässä tutkimuksessa mahdollisiksi suomalaisen valmistavan teollisuuden kyberturvallisuudelle tärkeiksi asioiksi vuonna 2021 nousi delfoin ensimmäisellä kierroksella 31 erilaista asiaa, jotka on listattu liitteeseen 5.

Toisella kierroksella näistä asioista jokainen asiantuntijapanelisti valitsi kaikista tärkeimmät ja vähiten tärkeimmät - ajatellen edelleen juuri suomalaisen valmistavan teollisuuden kyberturvallisuutta vuonna 2021. Seuraava kuva 4.2 havainnollistaa, kuinka valinnat jakautuivat eri asioiden kesken.




***Kuva 4.2*** *Suomen valmistavan teollisuuden kyberturvallisuuteen vaikuttavia asioita vuonna 2021.*

Kuten kuvasta 4.2 näkyy, asiantuntijapaneeli ei ollut mitenkään täysin yksimielinen asioiden tärkeydestä. Muutama asioista nousi kuitenkin tärkeydessä asiantuntijapaneelin suosikeiksi. Seuraavassa esitellään tarkemmin asiantuntijapanelistien näkemyksiä ja perusteluja valita juuri tietyt asiat tärkeimmiksi ja tietyt vähinten tärkeimmiksi - unohtamatta tietenkään mielipiteitä jakaneita asioita, joiden perusteluissa

tavattiin delfoille tunnusomaisia erimielisyysargumentteja [32].

## 4.4 Tärkeää vuonna 2021

Kuvasta 4.3 erottaa selvästi, että *IoT ja digitalisoituminen* ovat vuonna 2021 tärkeitä suomalaisen valmistavan teollisuuden kyberturvallisuuteen vaikuttavia asioita. Samalle aihealueelle kuuluu myös kohta *automaation turvallisuus*, jonka neljä asiantuntijoista näki tärkeäksi suomalaisen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021. Yhtä vaille kaikki panelistit valitsivat omalle tärkeimpien asioiden listalleen jommankumman kohdan joko *IoT ja digitalisoituminen* tai *automaation turvallisuus*. Kaksi panelisteista valitsi jopa molemmat.


***Kuva 4.3*** *Tärkeitä asioita Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021.*

*Teollisuusautomaation kyberturvallisuuteen* paneeli kertoi vaikuttavan esimerkiksi kyseisten laitteiden ja järjestelmien suuri koko ja pitkät elinkaaret, jotka vaikeuttavat niiden ajantasaista suojaamista. Hyökkääjät panelistit näkivät tässä kilpajuoksussa nopeammin liikkuviksi. Paneeli mainitsi myös, että laitteita ei ole suunniteltu ketterää IoT-kytkeytymistä varten, mutta kuitenkin esimerkiksi tietosuojan varmistaminen IoT- ja digitalisaatiohankkeissa on välttämätöntä. Useampi panelisti näki ongelmana vauhdin, jolla esimerkiksi IoT:n ja teollisen internetin uusia asioita halutaan saada toimimaan. Tällöin turvallisuudesta ei useinkaan ehditä huolehtimaan kunnolla.

Edellisten lisäksi trendiksi ja Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021 tärkeäksi asiaksi tutkimuksessa nousi *identiteettien ja pääsynhallinta*.

Yksikään panelisti ei valinnut sitä vähiten tärkeisiin, mutta sen sijaan neljä valitsi tärkeäksi (ks. kuva 4.3). Sen sijaan *identiteettivarkauksia*, jotka kuitenkin mainitaan kirjallisuudessa [11] valmistavankin teollisuuden ongelmaksi, ei kukaan ollut valinnut tärkeäksi Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021. Lisäksi vaikka *identiteettivarkaudet* tulivat myös esille ensimmäisellä kierroksella, niin yksi panelisteista koki sen jopa kuuluvan vähemmän tärkeiden asioiden joukkoon.

*Identiteettien ja pääsynhallinnan* osalta paneeli näki, että vaikka yritysten oman henkilöstön identiteetit ovat todennäköisesti jo kunnossa vuonna 2021, niin sen sijaan haasteena tulee yhä enemmän olemaan kolmansien osapuolien identiteetit ja pääsynhallinta. Jokaisen yrityksen on tärkeä pystyä hallitsemaan muun muassa alihankkijoidensa, asiakkaidensa ja toimittajiensa identiteettejä ja pääsyä, sillä yhä useammin myös nämä ryhmät toimivat yrityksen järjestelmissä ja käsittelevät kriittistä tietoa. Lisäksi paneeli huomautti, että identiteetit eivät enää välttämättä viittaa ihmisiin, vaan IoT:n yleistyessä myös erilaiset laitteet tulevat autentikoitumaan yrityksen verkkoon. Yksi panelisti sanoi "pääsynhallinnan olevan yksi haastavimmista asioista automaatiopuolella".

Paneeli koki *kolmansien osapuolien kyberturvallisuuden tason ja hallinnoinnin* tärkeäksi asiaksi Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021. Panelistit kuvasivat sitä kriittiseksi ja haastavaksi asiaksi, jonka suhteen "ei oikein edes tiedetä mitä pitäisi tehdä". Tämä kytkeytyy myös edelliseen, sillä tulevaisuudessa yhtenä tärkeänä haasteena nähdään juuri kolmansien osapuolien identiteettien ja pääsynhallinta. Yksi asiantuntija sanoi kolmansien osapuolien ja toimittajaketjun hallinnan olevan yksi tärkeimmistä oman yrityksensä kyberturvallisuuden tulevaisuuden kipupisteistä. Eräs panelisti muistutti niin ikään asian toisesta puolesta: myös heidän yrityksensä on monille se kolmas osapuoli, jonka tietoturvasta ja esimerkiksi identiteettien hallinnasta ollaan huolissaan. Tämä näkökulma tuo mukaan tarpeen todistaa yrityksen oman kyberturvallisuuden taso kumppaneille esimerkiksi juuri asiakkaille.

Aiheeseen liittyy myös ensimmäiseltä kierrokselta toiselle nostettu väittämä, että *asiakkaat tulevat kyllä kysymään, voiko yritykseemme luottaa ja tämä tarvitsee heille jotenkin todistaa.* Suurin osa panelisteista oli väittämän kanssa samaa mieltä ja näki, että sen merkitys myös kasvaa tulevaisuudessa. Vain kaksi panelisteista sanoi, että vaikka asia on erittäin tärkeä, se ei heidän asiakkailleen ole niin ajankohtainen. Toinen heistä kuitenkin totesi itse kysyvänsä tätä omilta toimittajiltaan ja lisäsi

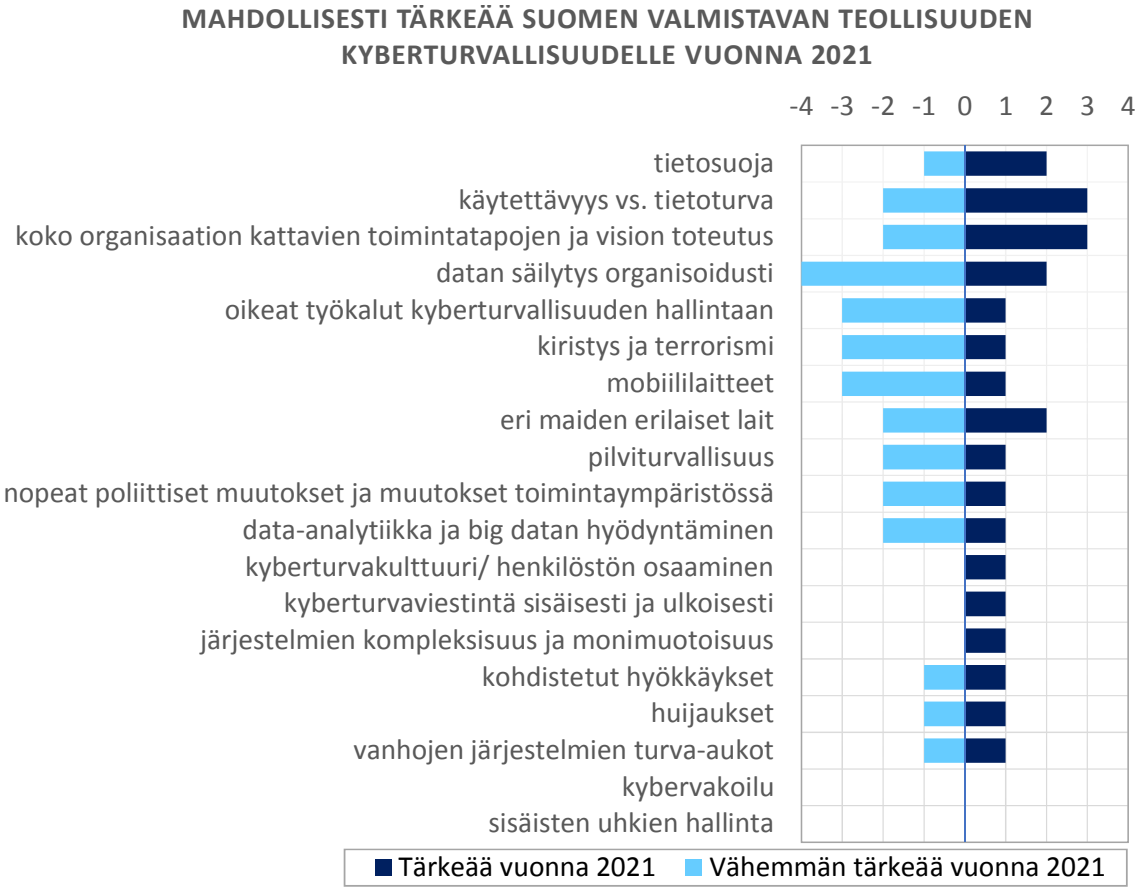
sijoittajien myös olevan aiheesta kiinnostuneita.

Näin ollen tähän väittämään voisi vaihtaa asiakkaat-sanan tilalle sanan sidosryhmät. Tällöin väittämä ei enää rajaisi ulkopuolelleen sijoittajien lisäksi esimerkiksi viranomaisia tai muita tahoja, joihin yrityksen toiminta vaikuttaa. Eräs panelisti näki, että väittämään sisältyvä luotettavuus liittyy myös yrityksen maineeseen ja muutama asiantuntija mainitsi sertifiointivalmiuden tärkeänä apuna oman kyberturvallisuuden todistamisessa asiakkaille. Ilmiö koettiin myös suhteellisen uudeksi valmistavassa teollisuudessa, ja eräs asiantuntijoista sanoikin, että "on tullut jo kysymyksiä, että onko teillä sertifikaattia - ei tällaista ole ennen valmistavalta yritykseltä kysytty".

Kuten kuvasta 4.3 huomaa, edellisten lisäksi useat panelistit näkivät *saatavuuden varmistamisen* selvästi enemmän tärkeänä kuin vähemmän tärkeänä asiana Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021. Panelisteista neljä valitsi sen tärkeäksi ja vain yhden panelistin mielestä se oli vähemmän tärkeää. Muista eriävän mielipiteen antaneen panelistin mielestä asiaan on jo kiinnitetty niin paljon huomiota, että vuonna 2021 se ei ole enää ole niin tärkeää. Ne, jotka kokivat saatavuuden varmistamisen tärkeänä, sanoivat, että asia ei muutu mihinkään: esimerkiksi kaikki katkot toiminnassa on edelleen oltava suunniteltuja.

## 4.5 Mahdollisesti tärkeää vuonna 2021

Tutkimuksessa tuli esille myös paljon erilaisia kiinnostavan ristiriitaisia näkemyksiä suomalaisen valmistavan teollisuuden kyberturvallisuuden tulevaisuuden painopisteistä. Osaan asioista ristiriitaisuutta toi se, mitä asiantuntijat puhuivat haastatteluissa verrattuna heidän vastauksiinsa haastattelujen välissä annetussa tehtävässä. Toisissa ristiriitaisissa asioissa eri panelisteilla oli vastakkaisia mielipiteitä näkemyksissään asian tärkeydestä. Nämä Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021 ristiriistaiset, eli mahdollisesti tärkeät, asiat näkyvät kuvassa 4.4.




***Kuva 4.4*** *Mahdollisesti tärkeitä asioita Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021.*

Panelistit saattoivat myös tulkita ensimmäisellä kierroksella kootun listan asioita ja termejä hieman erilailla, jolloin ristiriitaa ja näkemyseroja oli havaittavissa myös sen takia. Lisäksi tutkimuksessa mukana olevien panelistien taustat eroavat toisistaan ja heidän työnantajansa ovat erilaisia. Näin ollen panelistien valintoihin ja käsitykseen termeistä vaikuttavat esimerkiksi oma työhistoria sekä työnantaja-organisaation koko, asiakkaat ja strategia.

### 4.5.1 Datan suojaus

Dataan, sen suojaamiseen ja säilytykseen liittyi vahvasti kolme kohtaa kuvassa 4.4: *pilviturvallisuus*, *datan säilytys organisoidusti* sekä *tietosuoja*. Viimeisimmän suomalaisen valmistavan teollisuuden kyberturvallisuuden tärkeäksi vuonna 2021 nimesi kaksi henkilöä, mutta yksi uskoi asian olevan jo kunnossa silloin. Tärkeänä asian

kokeneet sanoivat, että valmistava teollisuus on edelleen niin sanotussa digitalisoitumisvaiheessa, jossa tietosuojaa ei olla ajateltu tarpeeksi: ei tiedetä, "missä data liikkuu tai missä ihmiset liikkuvat".

*Datan säilytys organisoidusti* oli kuuden eri panelistin listalla: kahden mielestä se on tärkeää vuonna 2021 suomalaisen valmistavan teollisuuden kyberturvallisuudelle ja neljän mielestä vähemmän tärkeää. Näin ollen tärkeys kallistuu hieman vähemmän tärkeän puolelle, jota eräs panelisteista perusteli näin: "Tämä korjaantuu jonkin verran GDRP:n myötä, eikä dataa enää oikein voida bunkkeroida, vaan se tulee olemaan helposti saatavissa ja sitä tulee olemaan kaikkialla." Yksi panelisti myös sanoi, että "tähän on jo välineitä ihan riittävästi". Asian tärkeäksi nähneet sanoivat sen olevan haasteellista esimerkiksi silloin, kun tiedon luokittelu nähdään osaksi sitä. Paneelin mukaan hankaluuksia tulee aiheuttamaan muun muassa "datan hajautuminen ympäriinsä" yhä enemmän, jolloin "ei oikein tiedetä missä dataa on ja miten sitä tulee suojata".

*Pilviturvallisuuden* vain yksi panelisteista valitsi tärkeäksi ja kaksi vähemmän tärkeäksi asiakasi. Asian tärkeäksi valinnut panelisti myös hieman epäröi sen tärkeyttä, mutta päätyi kuitenkin valitsemaan sen listalleen. Hän näki, että pilvistrategia täytyy suunnitella huolellisesti ja olla kunnossa: "mitä viedään pilveen, miten ja kuinka asiaa valvotaan". Hän näki heterogeenisen pilviympäristön hallinnan haastavana ja toisaalta taas se, "kuinka saada kaikki pilven kyvyt käyttöön". Pilviturvallisuutta täytyy myös lähestyä sopimuksien kautta, mikä eroaa konesalien hallinnasta.

*Pilviturvallisuuden* vähemmän tärkeäksi valinneet asiantuntijat näkivät, että pilven ja sen turvallisuuden merkitys tulee toki lisääntymään, mutta isot pilvitoimittajat, kuten Microsoft, ovat hoitaneet asiat hyvin. Nähtiin, että vuonna 2021 tähän asiaan ei täydy enää panostaa niin paljon, vaan se on jo kunnossa.

Edellisten lisäksi dataan ja sen käsittelyyn liittyvä *data-analytiikka ja BigDatan hyödyntäminen* jakoi panelistien mielipiteitä. Yhden mielestä juuri data-analytiikkaa halutaan entistä enemmän ja se on tärkeää, kun taas kaksi panelisteista ei pitänyt tätä erityisen tärkeänä kyberturvallisuuden näkökulmasta.

### 4.5.2 Vanhojen ja monimutkaisten järjestelmien perintö

Vanhojen järjestelmien turva-aukkojen tärkeys sai yhden panelistin puolelleen kun taas toinen panelisti näki, että suomalaisen valmistavan teollisuuden näkökulmasta

asia ei ole tärkeä vuonna 2021. Panelisti, joka ei nähnyt tätä tärkeänä asiana vuonna 2021 sanoi, että "aika hoitaa asioita, kun osa vanhoista järjestelmistä kuoleekin ajan kanssa." Lisäksi hän näki, että tähän on "aika helppoja ratkaisuja tarjolla, esimerkiksi serverit eivät oletuksena lähetä dataa ulos, jos tähän ei erikseen anneta lupaa".

Myös muissa kohdissa delfoi-haastatteluja useat panelistit sivusivat aihetta ja silloin he mainitsivat sen yhtenä tulevaisuuden haasteista. Esimerkiksi delfoin ensimmäiseltä kierrokselta nousseen väittämän, *ongelmia syntyy, kun halutaan yhdistää vanha suljettu järjestelmä internetiin*, paneeli totesi toisella kierroksella todeksi. Panelistit näkivät tästä tyypillisenä esimerkkinä IoT:n, sillä siinä usein uutta ja internetiin verkottunutta tekniikkaa koitetaan yhdistää vanhaan tekniikkaan, joka ei alun perin ole tarkoitettu yhdistettäväksi ulkopuoliseen verkkoon eikä ainakaan ketterästi.

IoT:n lisäksi myös muun vanhan perinnön paneeli näki tässä relevanttina, esimerkkeinä annettiin muun muassa "palvelujen vienti pilveen", "SAPin integroiminen operatiiviseen teknologioihin esimerkiksi ICS:ään" ja "toiminnanohjausjärjestelmään vietävä käyttäjänhallinta". Joillekin panelisteista tämä oli tullut jo muutaman kerran eteen kolmansien osapuolien kanssa, esimerkiksi kun asiakkaan järjestelmät ovat vanhoja. Eräs panelisti totesikin, että toimittajana on usein vain sopeuduttava ja hyväksyttävä asiakkaiden järjestelmien mahdollinen turvattomuus.

Paneeli myös muistutti, että yleisesti valmistavan teollisuuden laitokset ovat suuria ja kompleksisia, ja ne on suunniteltu toimimaan kymmeniä vuosia. Tällöin aikakaan ei aina korjaa vanhoissa järjestelmissä olevia aukkoja kovin nopeasti. Yksi panelisti näki, että tilanne on tällä hetkellä enemmänkin se, että vanhoja järjestelmiä on jo yhdistetty internetiin eli virhe on jo tapahtunut ja nyt "perintöä pitäisi siivota pois". Nähtiin, että uusien järjestelmien käyttöönotossa mennään helposti mukavuus ja nopeus edellä, eikä turvallisuusasioita ehditä ottaa mukaan.

Vanhojen järjestelmien perintöön voi katsoa liittyvän myös ensimmäiseltä delfoi-kierrokselta toiselle nostettuun väittämään *"If it works, don't fix it" -malli ei ole enää tätä päivää*. Ilmeni, että erityisesti valmistavan teollisuuden tuotantoympäristöissä vanhojen järjestelmien perintö vaikuttaa vahvasti nykypäivän toimintaan. Yksi panelisteista muotoili asian niin, että "ostetaan järjestelmä eikä kosketa siihen sitten vuosiin -malli ei enää ole nykypäivää, vaan järjestelmiä on ylläpidettävä". Muu paneeli oli samaa mieltä. Yksi tosin lisäsi, että muutoksissa on hyvä myös huomioida se, onko järjestelmä millaisessa paikassa eli onko sillä kokonaiskuvassa

merkitystä.

Haastatteluissa ilmenikin, että usein vanha järjestelmä saattaa toimia näennäisesti ihan hyvin, mutta silti jarruttaa koko ympäristön kehitystä. Eräs panelisti muistuttikin, että tällaiset vanhat järjestelmät voivat synnyttää riippuvuusketjuja ja koko ympäristön muuttaminen alkaa jähmettyä. Toinen panelisti taas huomautti, että vaikka muutokset ovat tärkeitä, niin niissä pitää huomioida myös vanhojen järjestelmien hyvät puolet: mikä niissä toimii hyvin ja miksi.

Myös kuvan 4.4 kohdan *järjestelmien kompleksisuus ja monimuotoisuus* voi nähdä liittyvän vanhojen järjestelmien perintötaakkaan. Vain yksi panelisteista valitsi tämän tärkeäksi, mutta toisaalta taas kukaan ei valinnut tätä vähemmän tärkeäksikään. Yksi tämän tärkeäksi valinnut panelisti mainitsi, että "näihin panostaminen ei tuo yhtään revenueta ja näitä tulee olemaan - ja kun nämä vuotavat, niin lähes kaikki muu tekeminen on turhaa". Eräs panelisti mainitsi myös, että "vanhojen järjestelmien paikkaaminen ei ole kenenkään lempihommaa", joten se on vaikea saada tehdyksi.

Vanhat ja monimutkaiset järjestelmät paneeli koki ongelmaksi erityisesti valmistavassa teollisuudessa. Tästä kertoo myös ensimmäiseltä kierrokselta noussut väittämä, että *valmistavan teollisuuden kyberuhkakartalla on paitsi kaikki normaalit uhkat niin myös monimutkainen tuotantoympäristö logiikkalaitteineen*, jonka paneeli toisella kierroksella tunnisti validiksi. Tähän paneeli assosioi monia erilaisia asioita kuten digitalisaation ja industry 4.0:n sekä niiden mukana tulevat kyberturvallisuushaasteet, jotka liittyvät esimerkiksi etäyhteyksiin laitevalmistajille ja muuhun datan suojaamiseen. Toisaalta myös kyberturvallisuuskontrolleihin nähtiin tulevan yhä enemmän koneoppimista, sillä reaktionopeudesta tulee yhä tärkeämpää ja päätöksiä on tehtävä yhä nopeammin.

Edellisen väittämän yhteydessä eräs panelisti kertoikin, että tuotantolaitoksien auditoinneissa "totuus usein kolahtaa naamalle pahasti", kun tärkeät tietoturvakontrollit on unohdettu. Yksi panelisteista sanoikin, että oleellista olisi "löytää kultainen keskitie turvallisuuden ja tuottavuuden välille - tietoturvaa tehdään hyvin, kun ei estetä rahan tulemista sisälle".

### 4.5.3 Kyberturvakulttuurin muutos

Asiantuntijapaneeli tunnisti, että tällä hetkellä kyberturvallisuus koetaan edelleen melko uudehkona asiana. Kuitenkin vähitellen siitä on tulossa yhä arkipäiväisempää ja se on siirtymässä osaksi kaikkea toimintaa myös valmistavassa teollisuudessa. Uskottiin, että vuonna 2021 Suomessa kyberturvallisuudelle olisi käynyt vähän samaan tapaan kuin aikoinaan liikenneturvallisuudelle: ensin ehkä vaikealtakin tuntuneeseen asiaan lopulta totutaan ja vähitellen se aletaan ottaa itsestään selvänä osana jokapäiväistä toimintaa.

Kyberturvallisuuden arkipäiväistymiseen liittyy myös vahvasti yrityksien kyberturvakulttuurin kehittyminen. Tämän suhteen panelistit näkivät monenlaisia muutoksia, mutta yleisen ymmärryksen kyberturvallisuudesta paneeli näki paranevan seuraavan viiden vuoden aikana. Kyberturvakulttuurin muutoksessa kriittisiksi vaikuttavaksi tekijöiksi annettiin esimerkkeinä esimiestoiminta ja koko henkilöstön, myös tuotannon, osaaminen sekä sitoutuminen. Eräs panelisti muistutti, että kyberturvakulttuurin on helpompi kehittyä, kun ihmiset tulevat törmäämään kyberturvallisuusasioihin ihan kotonaankin.

Lisäksi kyberturvakulttuurin myönteiseen suuntaan kehittämisessä paneeli piti tärkeänä, että kaikille yrityksessä tehdään selväksi, miksi jotkin kyberturvallisuuskontrollit ovat olemassa ja miksi heidän henkilökohtainen panoksensa on välttämätöntä kyberturvallisuuden onnistumiselle. Panelistit näkivät, että jos ihmiset eivät ymmärrä syytä, miksi heidän täytyy tehdä jokin ehkä käytettävyyttä huonontava asia, niin he saattavat vastustaa sitä tai yrittää ohittaa sen.

Kuvan 4.4 kohta *käytettävyys vs. tietoturva* jakoi asiantuntijoiden mielipiteitä: kaksi asiantuntijoista valitsi sen vähemmän tärkeäksi vuonna 2021 suomalaisen valmistavan teollisuuden kyberturvallisuuden näkökulmasta, mutta kolme taas ajatteli sen nimenomaan tärkeäksi kyberturvallisuusasiaksi vuonna 2021. Yksi asiantuntijoista sanoi, että asia ei enää ole tärkeä, koska siitä on jo päästy yli ja kulttuuri on muuttunut siten, että käytettävyyden huonontuminen kyberturvallisuuden takia hyväksytään. Sen sijaan eräs asian tulevaisuuden tärkeäksi valinnut panelisti perusteli kantaansa sillä, että esimerkiksi automaatiopuolella suorituskyky voittaa aina, eivätkä tiukat tietoturvakontrollit ole mahdollisia. Tällöin näissä ympäristöissä, joissa tuotanto ei voi seisahtua, käytettävyyden ja tietoturvallisuuden tasapainottaminen on haasteellista myös vuonna 2021.

Edelliseen liittyy läheisesti vielä myös yksi paneelin toisella delfoi-kierroksella todeksi toteama väittämä: *tietoturvalla ei saa kiusata – on huomioitava ihmiset*. Paneeli katsoi, että väittämä ei kuitenkaan tarkoita sitä, etteikö tietoturva saisi näkyä - joskus sen on jopa hyvä näkyä, sillä tällöin ihmiset muistavat sen tärkeyden. Tässäkin esille tuli näkemys, että ihmisten tulee ymmärtää, että kiusaamisen sijaan tietoturva suojelee ihmisiä ja heidän työtään. Tämän ajattelun edistäminen on tärkeää organisaatioiden kyberturvakulttuurin muutoksessa. Lisäksi paneeli näki, että vaikka tietyt asiat tietoturvasta on hyvä olla käyttäjille näkymättömiä, niin esimerkiksi näkyvä kaksivaiheinen autentikointi luo luottamusta.

Edellisen väittämän yhteydessä paneeli keskusteli myös kyberturvallisuuden merkityksestä, tehtävästä ja toiminnasta organisaatiossa: panelistit näkivät, että tulevaisuudessa kyberturvallisuuden pitäisi olla yhä konsultoivampaa, eikä enää niinkään autoratiivista. Eräs panelisti mainitsikin, että kun huomioidaan ihmiset eikä kiusata heitä tietoturvalla, niin yleensä samalla on huomioitu myös liiketoimintaprosessit. Moneen ongelmaan uskottiin auttavan, jos liiketoiminta osallistetaan kyberturvallisuustyöhön.

Tästä huolimatta muutama panelisti kuitenkin muistutti, että myös tulevaisuudessa tulee edelleen eteen, jolloin on sanottava "jämäkkä ei". Silloin on tärkeää, että "ei" perustellaan ymmärrettävästi liiketoiminnalle. Sillä jos liiketoiminta ei ymmärrä kieltoa, niin se saattaa ohittaa sen - päätös on lopulta kuitenkin liiketoiminnalla.

Lisäksi kyberturvallisuuskulttuurin positiivisessa muutoksessa paneeli näki tärkeänä hyvän keskustelun fasilitoiminen paitsi omassa organisaatiossa niin myös asiakkaisiin ja julkisuuteen päin. Eräs panelisti mainitsikin, että harva ihminen missään yrityksessä haluaa oikeasti olla välinpitämätön kyberturvallisuuden suhteen, kunhan vain tietää, mitä riittävän turvallisuuden varmistamiseksi täytyy tehdä. Pelkkien "lue tietoturvapolitiikka" -tyylisten käskyjen sijaan käytännön ohjeet nähtiin tärkeinä ihmisten ja liiketoiminnan sitouttamiseksi.

Samassa kuvassa kohdan *kyberturvakulttuuri/henkilöstön osaaminen* oli valinnut tärkeäksi panelisteista vain yksi, mutta toisaalta kukaan ei ollut listannut sitä vähemmän tärkeäksikään. Samoin yksi panelisti oli valinnut tärkeäksi kyberturvakulttuuriin vahvasti liittyvän *ulkoisen ja sisäisen kyberturvaviestinnän*. Priorisoinnin tuloksiin (kuva 4.4) verrattuna hieman ristiriitaisesti monet panelisteista kuitenkin mainitsivat kyberturvallisuuskulttuurin kehittämiseen liittyviä asioita muutoin haastatteluissa. Näitä tuli esille esimerkiksi kysyttäessä yrityksensä kyberturvalli-

suuden tulevaisuuden "kipukohtia" tai kyberturvallisuusasioita, jotka on hoidettava seuraavan viiden vuoden aikana. Suurin osa muun muassa suunnitteli lisäyksiä henkilöstön koulutukseen ja koki tämä asiat tärkeäksi.

Asiantuntijapaneeli oli yksimielinen, että ensimmäiseltä delfoi-kierrokselta toiselle nostettu, kyberturvakulttuuriin läheisesti liittyvä väittämä, että *turvallisuusvaatimus täytyy integroitua kaikkeen tekemiseen*, on totta. Integroituminen kaikkeen toimintaan on kuitenkin mahdollista vasta, kun tietoturvakulttuuri on saatu tarpeeksi hyvälle tasolle, kuten eräs panelisteista sanoikin: "tietoisuuden tason on istuttava tekemiseen, ihmiseen ja prosesseihin".

Turvallisuusvaatimusten integroitumisesta panelistit antoivat esimerkkeinä muun muassa kolmansien osapuolien sopimuksissa mukana olevat tietoturvavaatimukset sekä projektimalleissa mukana olevat kyberturvallisuusportit. Tähän suuntaan ollaan jo nyt selvästi menossa - esimerkiksi yksi panelisteista kertoi, että jokin aika sitten heidän käyttämäänsä projektimallin perusoletuksiin oli otettu "kyberturvallisuusportti"mukaan, mikä tarkoittaa kyberturvallisuuden omaa oletusaskelta tai tarkastusta projektimallin mukaisessa prosessissa.

Kyberturvakulttuuriin ja projekteihin liittyy myös ensimmäiseltä kierrokselta toiselle nostettu väittämä, että *meillä ei ole tietoturvaprojekteja - meillä on liiketoiminnan projekteja, joissa tietoturva on mukana*, jonka melkein jokainen panelisti tunnisti todeksi. Yksi panelisti tiivisti, että "kyberturvan tulisi olla luontainen osa projekteja" ja toinen lisäsi, että "liiketoiminnan edustus ja omistajuus tarvitaan mukaan". Muutama panelisteista huomautti, että tällä hetkellä kyberturvallisuus otetaan mukaan projekteihin liian myöhään - osittain myös omasta syystä, sillä "usein tietoturva pyytää kuitenkin jo jotain valmista ja evidenssi tehdään myöhään".

Yksi panelisti kuitenkin hieman haastoi edellistä väittämää: "Kyllä niitä on ihan pelkkiä tietoturvaprojektejakin esimerkiksi, jos palomuureja vaihdetaan, niin se on tietoturvaprojekti."Hän kuitenkin lisäsi: "Mutta toki ajatus tässä takana on tärkeä ja oikein, että tietoturva on projekteissa mukana alusta asti." Lisäksi toinen panelisti kertoi asian kyllä olevan näin yrityksen sisäisissä projekteissa, mutta "kun myydään ulospäin tuotteita ja palveluita, niin sitten ei siinä sitten [kyberturvallisuus] ole niin hyvin mukana - odotetaan, että ostavalla osapuolella on valmius evaluoida". Kolmas panelisti näki, että projektien sijaan "on oltava olemassa jatkuva ohjelma, sillä homma ei projekteilla pysy kasassa - jonkinlainen kyberturvan vuosisykli, joka poikii sitten projekteja".

Useampi panelisteista korosti kyberturvakulttuurin muutokselle tärkeäksi, että kaikki ymmärtävät kyberturvallisuuden olevan jokaisen asia eikä vain esimerkiksi IT:n. Kuitenkin tällä hetkellä käytännön tasolla suomalaisen valmistavan teollisuuden yrityksissä kyberturvallisuus näyttäisi useimmiten olevan tietoturvajohtajan vastuulla ja organisatorisesti sijoitettuna tietohallintojohtajan alaisuuteen osaksi IT:tä. Muutamassa yrityksistä tämän lisäksi raportoidaan myös riskienhallinnalle ja joidenkin panelistien mielestä kyberturvallisuus kuuluisikin enemmän juuri sinne. Suurin osa panelisteista näki, että kyberturvallisuuden organisointiin ja vastuunjakoon on tulossa muutoksia seuraavan viiden vuoden aikana, ja sekä riskienhallinnalle että liiketoiminnalle tullaan siirtämään yhä enemmän kyberturvallisuusvastuita.

Paneeli keskusteli kyberturvakulttuurin muutoksesta myös ensimmäiseltä kierrokselta toiselle nousseen väittämän *yksi koko ei enää sovi kaikille* yhteydessä. Panelistit näkivät, että kyberturvallisuuden hallinnassa on otettava yhä paremmin huomioon organisaation eri alikulttuurit: kaikkialla eivät samat keinot toimi. Lisäksi muistutettiin hyökkäyskohteiden kiinnostavuudessa olevan eroja, jotka on huomioitava niiden suojaamisessa. Eräs panelisti mainitsikin, että Suomen valmistava teollisuus on vähän liian "luottavaisessa turvallisuuden tunteessa", mutta on vain ajan kysymys, milloin jokin hyökkäävä taho kiinnostuu juuri suomalaisista yrityksistä. Yksi panelisteista toi tähän myös tietoturvapalveluiden hankinnan näkökulmaa: "Eri yrityksien pitäisi ymmärtää hankkiessaan palveluita, myös tietoturvapalveluita, että tarvitsee olla toimittajalle sopivan kokoinen – isolle saattaa olla liian pieni, pienemmälle taas on merkittävä asiakas."

*Yksi koko ei enää sovi kaikille* -väittämä voidaan yhdistää myös toiseen ensimmäiseltä delfoi-kierrokselta toiselle nousseeseen väittämään: *täytyy tietää mitä suojelee, siitä kaikki lähtee*. Tällöin on huomattava, että eri yrityksissä erilaiset asiat ovat tärkeitä suojella. Nähtiin, että kun kaikkea ei voi suojella samalla painoarvolla, on kyberturvallisuuden rajalliset resurssit kriittistä pystyä kohdentamaan oikein. Joissakin yrityksistä oli selvitetty yrityksen niin kutsutut kruunun jalokivet eli varat, joiden suojaaminen on kaikista tärkeintä. Toisissa yrityksissä näiden tunnistaminen oli joko kesken tai suunnitteilla tehtäväksi lähiaikoina.

Kruunun jalokivien lisäksi eräs panelisti yhdisti tähän myös tiedon luokittelun, jonka tarkoitus on selventää kaikille, kuinka huolellisesti mikäkin asia tulee suojata. Tätä tietoa kruunun jalokivistä sekä tiedon luokittelua tarvitsee myös ylläpitää, sillä kuten yksi panelisteista mainitsi, yrityksen suojauksen tärkeysjärjestys muuttuu

kokoajan: "Mitä suojeltiin viisi vuotta sitten on ihan erityyppistä kuin mitä viiden vuoden päästä tai nyt." Paneeli näki myös, että uuden tietosuoja-asetuksen myötä tärkeiden tietojen suojaaminen saa hyvää näkyvyyttä, kun kaikkien organisaatioiden on selvitettävä, mitä tietoa heillä on ja missä se sijaitsee.

Kyberturvakulttuuriin liittyy myös vahvasti se, ymmärtääkö yrityksen henkilökunta kyberturvallisuuden arvon liiketoiminnalle vai nähdäänkö koko kyberturvallisuus mahdollistajan sijaan lähinnä hidasteena. Tämän paneeli näkin parantuneen viime aikoina, mutta silti huomautettiin, että vielä tehtävää riittää. Yksityisyyden suojan tärkeys yleensä ymmärretään ja suhtautuminen kyberturvallisuuteen on muuttunut positiivisemmaksi. Paneeli kuitenkin mainitsi, että näkemykset varmasti vaihtelevat paljon jokaisen yrityksen sisällä, eikä yhtenäistä kyberturvallisuuskulttuuria ole. Eräs panelisti sanoi, että "henkilöstö ei ehkä näe kovinkaan paljon arvoa liiketoiminnalle, mutta ymmärtää turvaamisen olevan tärkeää kilpailullisen etulyöntiaseman säilyttämiseksi - eli toisin sanoen ei haluta hukata tehtyä työtä, jolla on arvo".

Toisaalta hyvän kyberturvakulttuurin omaavassa organisaatiossa myös keskeiset kyberturvallisuustoimijat ymmärtävät yrityksen ydinliiketoimintaa. Yleisesti useissa tutkimuksen yrityksissä tuotanto oli fyysisesti lähellä kyberturvallisuustoimijoita, jolloin heidän ymmärryksensä tuotannon arkipäivästä on hyvää. Lisäksi valmistavalle teollisuudelle tyypillisten pitkien työurien mainittiin auttavan siinä, että kyberturvallisuustoimijat ovat sisäistäneet yrityksen ydinliiketoiminnan. Eräs panelisti mainitsi myös oman, sisäisen IT:n hyödyllisenä, sillä se tuntee yrityksen prosessit, ymmärtää saatavuuden tärkeyden liiketoiminnalle ja sijaitsee lähellä. Yksi asiantuntija huomautti, että "toisen tavoitteiden ja työn ymmärtäminen ei ehkä koskaan ole täydellistä". Tästä huolimatta tätä ei kuitenkaan nähty tulevaisuudessakaan erityisenä ongelmana Suomen valmistavassa teollisuudessa.

Viimeiseksi kyberturvakulttuuriin voidaan katsoa liittyväksi myös kohta *koko organisaation kattavien toimintatapojen ja vision toteutus*, joka myös jakoi panelistien mielipiteitä: kolme piti sitä tärkeänä Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuuden näkökulmasta, kun taas kaksi piti sitä vähemmän tärkeänä. Tärkeäksi sen valinneet näkivät sen kytkeytyvän koko organisaation kulttuurin kääntämiseen, joka erään panelistin sanoin "ei ole vain IT:n juttu". Kulttuurimuutokseen sitouttamiseen nähtiin tarvittavan vahvaa päätöksentekoa sekä erityisesti keskijohdon sitoutumista.

Ne, joiden mielestä *koko organisaation kattavien toimintatapojen ja vision toteu-*

*tus* ei ollut tärkeää Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021, perustelivat näkemystään sillä, että asia on nyt käynnissä ja sen pitäisi olla jo kunnossa vuonna 2021. Hekin kuitenkin näkivät, että onnistuminen vaatii koko organisaation osallistumista ja sitoutumista. Yksi panelisti olikin työssään usein miettinyt, että "kuinka saada toimivia koko organisaatiolle sopivia ratkaisuja, jotka eivät ole liian jäykkiä käytettäväksi".

### 4.5.4 Muuta mahdollisesti tärkeää

*Eri maiden erilaiset lait* -kohdasta asiantuntijoilla oli erilaiset näkemykset: kaksi piti tärkeänä ja kaksi vähemmän tärkeänä. Asiantuntijat näkivät, että asia ei ole enää 2021 kovin tärkeä koska "nämä tulevat annettuna"ja "näkyy toki tietosuojapuolella ja tuotepuolella, muttei ehkä valmistavassa teollisuudessa nyt niin iso asia". Asian tärkeyttä vuonna 2021 suomalaisen valmistavan teollisuuden näkökulmasta puolusti näkemys, että toiminta on yhä kansainvälisempää erityisesti suurissa yrityksissä ja kaikkien maiden lakeja täytyy noudattaa.

*Kohdistettujen hyökkäyksien* ja *huijauksien* tärkeydestä paneeli ei myöskään ollut yhtä mieltä. Molemmat saivat yhdet äänet kumpaankin suuntaan. Kohdistetut hyökkäykset tärkeiksi valinnut panelisti perusteli näkemystään, että "jos kohdistettu hyökkäys osuu kriittisiin komponentteihin, niin monissa yrityksissä pariin kohtaan hyökkääminen riittää". Vähemmän tärkeänä asian nähnyt oli sitä mieltä, että kohdistetuista hyökkäyksistä tulee vuonna 2021 jo "normaalia"rikollisuutta eivätkä ne ole kenellekään enää mitenkään ihmeellisiä. Sekä huijauksissa että kohdistetuissa hyökkäyksissä paneeli näki edelleen vuonna 2021 rahan ja tiedon olevan hyökkääjien tärkeimmät motiivit.

Paneelin mielipide *mobiililaitteiden* tärkeydestä suomalaisen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021 kääntyi hieman siihen suuntaan, että asia ei olisi enää tärkeää vuonna 2021 (ks. kuva 4.4). Tätä mieltä oli kolme panelistia kun taas yksi oli sitä mieltä, että mobiililaitteet ovat "totta kai listalla, sillä tähän maailma menee - tulevaisuudessa ei voida enää kontrolloida laitteita". Vähemmän tärkeiksi mobiililaitteet sijoittaneet sanoivat, että "työasemissa on enemmän aukkoja kuin mobiililaitteissa"ja että "mobiililaitteet kehittyvät ja tämä on jo neljässä vuodessa ratkaistu".

*Kiristys ja terrorismi* -kohta jakoi myös mielipiteitä, mutta yhteenlaskettuna sitä

pidettiin hieman enemmän vähemmän tärkeänä kuin tärkeänä: kolme panelistia piti vähemmän tärkeänä ja yksi tärkeänä (ks. kuva 4.4). Tärkeänä asiaa pitänyt panelisti sanoi kiristykseltä puolustautumisen olevan tärkeää, sillä esimerkiksi kiristyshaittaohjelmat tulevat vain lisääntymään entisestään. Vähemmän tärkeäksi asian nähneet sanoivat, että vaikeasti se on vaikeasti hallittava, sillä esimerkiksi terrorismissa vastassa on yleensä isoja toimijoita epäselvine motiiveineen. Tätä pidettiin myös vain uutena rikollisuuden muotona, johon ei tule eikä oikein voidakaan resurssien puolesta keskittyä.

Suomalaisen valmistavan teollisuuden kyberturvallisuuden tärkeäksi ei yltänyt myöskään *nopeat poliittiset muutokset ja muutokset toimintaympäristössä* -kohta. Vain yksi panelisti valitsi kyseisen kohdan tärkeäksi ja kaksi valitsi sen vähemmän tärkeäksi (ks. kuva 4.4). Toinen asian vähemmän tärkeäksi valinneista panelisteista sanoi, että jos jotain tällaista osuu kohdalle, niin "se sitten vain otetaan vastaan, sillä asiaa on vaikea ennustaa". Eräs panelisti taas huomautti, että tämä kohta on tärkeämpi, jos yrityksellä on toimintaa Kiinassa tai Venäjällä.

Kuten kuva 4.4 kertoo, kybervakoilua tai sisäisten uhkien hallintaa kukaan panelisteista ei listannut erityisen tärkeäksi suomalaisen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021. Toisaalta, näistä kumpaakaan kukaan ei listannut myöskään vähemmän tärkeäksi. Sen sijaan panelistit kyllä mainitsivat nämä molemmat muissa kohdissa haastatteluita. Esimerkiksi muutama mainitsi suoraan, että teollisuusvakoilijat saattavat uhata yrityksen kyberturvallisuutta vuonna 2021. Nämä asiat voivat siis olla tulevaisuudessa tärkeitä Suomen valmistavan teollisuuden kyberturvallisuudelle, mutta niiden tärkeyttä ei vielä laajasti nähdä.

## 4.6 Vähemmän tärkeää vuonna 2021

Alla olevaan kuvaan 4.5 on koottu asiat, jotka ovat vuonna 2021 suomalaisen valmistavan teollisuuden yritysten kyberturvallisuuden hallinnassa vähemmän tärkeitä. Melkein jokainen asiantuntijapanelin jäsen sanoi, että vähemmän tärkeiden asioiden valitseminen oli paljon haastavampaa kuin tärkeiden. Lisäksi korostettiin, että "vähemmän tärkeä" ei tarkoita, että asian saisi pyyhkiä kokonaan pois mielestään, vaan kaikki listan asiat ovat edelleen vuonna 2021 osa kyberturvallisuuden hallintaa. Nyt 4-5 vuoden aikana kuitenkin kyberturvallisuustekemisen painopisteet muuttuvat, kun kaikkeen aika ja muut resurssit eivät riitä.


***Kuva 4.5*** *Vähemmän tärkeitä asioita Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021.*

Käytännössä tämä tarkoittaa sitä, että näiden vähemmän tärkeiksi valittujen asioiden hoitamiseen ei todennäköisesti enää vuonna 2021 käytetä niin paljon valmistavan teollisuuden kyberturvallisuuden resursseja. Sen sijaan ne voivat silloin tarvita esimerkiksi lähinnä enää vain ylläpitoa, sillä niihin on jo aikaisemmin panostettu niin paljon. Seuraavassa on esitelty tarkemmin panelistien valintoja ja perusteluja, miksi tietyt asiat eivät vuonna 2021 enää ole tärkeitä Suomen valmistavan teollisuuden kyberturvallisuudelle.

### 4.6.1 Kyberhyökkäyksien aiheuttamat maineuhkat

Suomalaisen valmistavan teollisuuden maineriskiä ja kyberturvallisuuden vaikutusta siihen tulevaisuudessa sivuttiin useammassa kohtaa tutkimusta. Asiantuntijapaneeli mietti esimerkiksi, voiko vuonna 2021 suomalaisen valmistavan teollisuuden maine olla uhattuna kyberhyökkäyksen takia ja kuinka todennäköistä se on. Kaikki asiantuntijat näkivät mahdollisena, että seuraavan viiden vuoden aikana kyberhyökkäys saattaa uhata heidän yrityksensä mainetta ja kaksi piti maineuhkaa jopa "sata prosenttisen varmana". Kolme yhdeksästä haasteltavasta tunnisti todennäköisyyden oman yrityksensä kohdalla pieneksi, mutta silti mahdolliseksi.

Delfoin ensimmäisellä kierroksella yksi asiantuntijoista toi esille maineriskiin läheisesti liittyvän väittämän: *mediassa lumipallo lähtee vyörymään nopeasti*. Toisella

kierroksella jokainen asiantuntija tunnisti tämän median valtaa, nopeutta ja voimaa kuvaavan väittämän todeksi ja oleelliseksi myös Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuuden näkökulmasta. Asiantuntijapaneelin mielestä myös vuonna 2021 asiat leviävät ja paisuvat mediassa nopeasti ja "isolla mittakaavalla", kuten eräs panelisteista asian ilmaisi. Erityisesti sosiaalinen median panelistit mainitsivat haastavaksi ja "mahdottomaksi kontrolloida".

Edellisistä huolimatta *maineriskien hallinnan* useimmat panelistit eivät nähneet olevan tärkeää suomalaisen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021 (ks. kuva 4.5). Sen sijaan riski luokiteltiin vähemmän tärkeäksi, sillä katsottiin sen olevan vuonna 2021 jo ymmärretty ja hallinnassa. Yksi asiantuntijoista myös katsoi maineriskien hallinnan kuuluvan enemmän muuhun riskienhallintaan kuin suoraan kyberturvallisuuden alueelle, vaikka kyberhyökkäys voikin uhata yrityksen mainetta.

Mitä enemmän yrityksellä on toimintaa suorassa kuluttajarajapinnassa, sitä todennäköisemmäksi, kriittisemmäksi ja haastavammaksi maineriski arvioitiin. Lisäksi nähtiin, että valmistavan teollisuuden muutos kohti palveluliiketoimintaa lisää riskin merkittävyyttä tulevaisuudessa. Henkilötietojen vuotaminen, yrityksen ympäristörikokseen liittäminen ja saatavuuteen vaikuttaminen tuotiin esille esimerkkeinä kyberhyökkäyksen seurauksista, jotka vahingoittavat yrityksen mainetta ja siten myös liiketoimintaa. Näiden lisäksi vakavaksi maineuhkaksi paneeli näki, jos yrityksen kyberturvallisuusongelmat haittaavat asiakasta - kuten esimerkiksi, jos asiakaan tietoja pääsee vuotamaan tai jos hyökkääjä pääsee yrityksen kautta käsiksi asiakkaan järjestelmiin.

Maineriskin merkittävyyttä voi pienentää varautumalla uhkiin ennakkoon: useampi asiantuntija mainitsi muun muassa hyvän ja ajantasaisen kriisiviestintäsuunnitelman tärkeyden. Uhkan toteutuessa tapauksen nopea ja avoin kommunikoiminen kaikille sidosryhmille koettiin myös hillitsevän eskaloitumista ja pienentävän uhkan vaikuttavuutta. Asian vakavuuteen vaikuttavat sekä julkisuuteen tulevan tapauksen sensitiivisyys että myös itse yrityksen tunnettavuus. Eräs panelisteista näki, että yritykset tulevat tulevaisuudessa käyttämään viestinnän seuraamiseen ja omaa yritystä koskevaan uutisointiin reagoimiseen yhä enemmän ulkopuolisia palveluita, sillä mitä nopeammin asia huomataan ja siihen reagoidaan, sitä vähemmän yrityksen maine vaurioituu. Yksi asiantuntija muistutti kuitenkin, että median vauhdikkuuden voi nähdä myös hyvänä asiana: negatiivisen lisäksi myös positiivinen viesti tavoittaa ison määrän kuulijoita helposti.

Lisäksi haasteltavista muutamat kertoivat jo nyt kohdanneensa esimerkiksi sosiaalisesta mediasta tulleita maineriskejä, jolloin siihen liittyvää kriisiviestintää on tullut jo harjoiteltua. Useammat myös mainitsivat, että heidän yrityksissään on jo kriisiviestintäsuunnitelmat mainetta uhkaavan kyberhyökkäyksen varalle. Näin ollen voidaan päätellä, että *maineriskien hallinta* (mukaan lukien *sosiaalinen media*) ei todennäköisesti ole niin tärkeää Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021.

### 4.6.2 Viranomaisyhteistyössä ei merkittäviä haasteita

Asiantuntijapaneeli vaikutti olevan sitä mieltä, että vuonna 2021 viranomaisyhteistyö ei tuo erityisiä haasteita suomalaisen valmistavan teollisuuden kyberturvallisuuden hallintaan. Eräs panelisti kuvasi keskustelun olevan avointa. Toki paneeli tiedosti, että viranomaiset, erityisesti Euroopan Unioni, ovat aktiivisia näissä asioissa myös jatkossa. Esimerkiksi tällä hetkellä panelistien yrityksissä mietitään, kuinka GDPR:ää (General Data Protection Regulation) tullaan tulevaisuudessa tulkitsemaan. Yksi asiantuntija kuitenkin uskoi, että koska GDPR tulee voimaan jo 2018 toukokuussa, niin "pelikenttä kirkastuu kaikille jo ennen vuotta 2021".

Erään panelistin mielestä viranomaisilta kuitenkin kaivattaisiin laajempia toimenpiteitä ja nyt keinoina tuntuu olevan vain säädösten ja vaatimusten lisääminen, jolloin vastuu sysätään yksin yrityksille tai yksityisille uhreille. Hän epäili myös, pysyykö lainsäätäjä nopeasti muuttuvien uhkien perässä: pystyykö reagoimaan ja uudistumaan tarpeeksi nopeasti. Kukaan asiantuntijoista ei kuitenkaan valinnut kohtaa *viranomaisyhteistyön haasteet* tärkeäksi ja kolme valitsi sen vähemmän tärkeäksi.

### 4.6.3 Ylin johto jo sitoutettu

Vaikka asiantuntijapaneeli näki ylimmän johdon sitoutumisen kriittisenä asiana kyberturvallisuuden onnistumiselle myös tulevaisuudessa, ei sitä enää nähty tulevaisuuden tärkeänä (ks. kuva 4.5). Delfoi-haastattelujen perusteella voidaan todeta, että panelistien yrityksissä ylin johto on kiinnostunut kyberturvallisuudesta ja esimerkiksi kyselee aiheesta. Kiinnostuksen uskotaan myös lisääntyvän tai pysyvän saavutetulla korkealla tasolla. Julkisuudessa esillä olevat kyberturvallisuustapahtumat pitävät aiheen johdon mielessä. Eräs panelisti sanoikin: "Kertaakaan en ole

törmännyt ongelmaan, että ei olisi otettu keskustelemaan tällä kyberteemalla [ylimmän johdon kanssa]." Tämän eteen on yrityksissä viime vuosina tehty paljon töitä ja panelistit uskovatkin, että vuonna 2021 kyberturvallisuuden resursseja kannattaa kohdistaa jo muualle. Lisäksi yksi panelisti muistutti, että tulevaisuudessa yrityksen johto nuorentuu, ja nuoremmille sukupolville kyberturvallisuus on tutumpi asia, joka pitää olla kunnossa.

Yrityksissä ylimmän johdon sitoutumisesta kertoo myös se, että asiantuntijoista melkein jokainen kertoi, että heidän yrityksensä viisivuotissuunnitelmiin on sisällytetty kyberturvallisuusaiheita. Kyber-sanaa ei kaikissa yrityksissä oltu välttämättä käytetty suoraan, mutta asiaa oltiin sivuttu tai siihen liittyviä turvallisuusaiheita, kuten luotettavuutta, oli nostettu esille. Lisäksi melkein kaikissa yrityksissä, tarkemmin sanottuna seitsemässä yhdeksästä, toimintaa ohjaamaan oli tehty kyberturvallisuusstrategia tai -visio. Lisäksi yhdelle yrityksistä oli tällainen tulossa lähiaikoina.

Kaikissa yrityksissä kyberturvallisuusaiheita oli sisällytetty yrityksen riskienhallintaan ja riskienhallintasuunnitelmiin. Jokaisessa yrityksessä oli myös tehty jonkinlainen riskikartoitus tai auditointi, jonka pohjalta kyberturvallisuutta lähestyttiin riskienhallinnan näkökulmasta. Riskien kartoittamiseen suosittu työkalu vaikutti olevan Information Security Forumin (ISF) Information Risk Assessment, jonka uusin versio Methodology 2 on kaikille ISF:n jäsenille vapaasti saatavilla internetistä [17].

Haastattelujen perusteella näyttää siis siltä, että suomalaisen valmistavan teollisuuden ylin johto on saatu sitoutettua kyberturvallisuuteen. Sitoutumista enemmän haasteeksi nähtiin, että "pystytäänkö tulkkaamaan ylimmälle johdolle, mitä mikäkin tarkoittaa juuri oman yrityksen liiketoiminnan kannalta". Lisäksi useampi haasteltava mainitsi, että seuraava haaste on sitouttaa keskijohto, jolla on suuri vaikutus yrityksen jokapäiväiseen operatiivisessa toiminnassa ja siten myös kyberturvakulttuurin muutoksessa.

### 4.6.4 Kyberturvallisuusresurssien riittävyys

Ylimmän johdon sitoutumisesta kyberturvallisuuteen kertoo myös se, että suurin osa asiantuntijapanelisteista ennakoi yrityksensä investoivan lisää kyberturvallisuuteen seuraavan 4-5 vuoden aikana. Eräältä asiantuntijalta oli yrityksen johto jopa kysynyt, onko kyberturvallisuuteen varmasti laitettu tarpeeksi rahaa. Vain kaksi panelisteista ei uskonut yrityksensä kyberturvallisuusinvestointien kasvavan nykyi-

sestä. Toinen heistä tosin jatkoi, että kyberturvallisuuteen on viimeiset pari vuotta investoitu suuresti ja tämän takia budjetin kasvattaminen edelleen on tuskin mahdollista. Hän kuitenkin näki, että investoinnit todennäköisesti pysyvät nykyisellä korkealla tasollaan.

Yksi panelisteista toi esille myös näkökulman, että valmistavan teollisuuden yrityksissä kyberturvallisuuteen panostaminen nähdään edelleen lähinnä vain kustannuksena eikä investointina - sen sijaan vastapuolelle eli hyökkääjille kaikki panostukset ovat aina investointeja. Samaa asiaa sivuaa myös ensimmäiseltä kierrokselta toiselle nostettu väittämä: *usein kysytään mitä tietoturva maksaa - pitäisi kysyä mitä maksaa toimimaton tunti*. Suurin osa panelisteista oli samaa mieltä - yksi tosin haastoi, että tämä ei aina ole oikea kysymys, sillä kyberturvaongelmien seuraukset voivat olla hyvin moninaisia. Toinen panelisti taas huomautti, että yksi haaste tässä on kyberturvallisuuden koostuminen useista eri muuttujista: monista muista investoinneista tiedetään, että ne poistavat jonkin vian kokonaan, mutta kyberturvallisuudessa se ei koskaan ole varmaa. Tämä ongelma ei myöskään helpota tarvittavista kyberturvainvestoinneista kommunikointia - erityisesti, kun monet asiantuntijoista tunnistivat kyberturvallisuuden olevan yrityksessään edelleen "hieman vierasta dialogia".

Kyberturvallisuusinvestointien yhtenä haasteena paneeli näkikin niiden hyödyllisyyden osoittamisen ja mittaamisen: mitä oikeastaan lasketaan kuuluvaksi kyberturvallisuuteen ja kuinka investointien tehokkuutta kyberturvallisuuden parantamisessa olisi edes mahdollista mitata? Hyvien mittarien koitteen kuitenkin olevan tarpeen, jotta voidaan esimerkiksi johdolle osoittaa kyberturvallisuuden merkitys ja toiminta. Monet panelisteista sanoivatkin, että heidän yrityksensä kyllä mittaa jotakin asiaa kyberturvallisuudesta, mutta kokonaisnäkymää investointien tehokkuuteen ei ole. Esimerkiksi useampi yritys saa tietoturvatapahtumien valvomoista raportteja, mutta niiden ei uskottu kertovan kaikkea. Eräs panelisteista sanoi, että "koska kyberturvallisuus on hankalasti mitattava ja sen hyödyllisyyttä on vaikea osoittaa, siitä ei ole helppo tehdä kilpailuvalttia tällä alalla".

Yksi panelisteista kertoi mittaamista hankaloittaneen myös sen kohtaama vastarinta: jotkut eivät pidä kyberturvallisuuden mittaamisesta, sillä se voi paljastaa heikkouksia omalta vastuualueeltaan. Kaikesta huolimatta *kyberturvallisuuden mittaamista* ei kukaan panelisteista valinnut tärkeäksi ja yksi jopa valitsi sen vähemmän tärkeiden asioiden joukkoon (ks. kuva 4.5).

Suomalaisen valmistavan teollisuuden kyberturvallisuuden *henkilöresurssien riittävyydestä* vuonna 2021 asiantuntijapaneeli ei ollut erityisen huolissaan. Kuten kuva 4.5 kertoo, kukaan panelisteista ei listannut tätä tärkeäksi, mutta kolme sanoi tämän olevan vähemmän tärkeää vuonna 2021. Paneeli koki, että kyberturvallisuus on tulevaisuudessa jo rakennettu enemmän yrityksen toimintoihin sisään ja osaksi jokaisen työntekijän työnkuvaa, jolloin juuri kyberturvallisuuden henkilöresurssit eivät ole enää kriittisiä.

Toki ongelma tunnistettiin ja haasteelliseksi eräs panelisti mainitsi esimerkiksi tilanteen, jossa yrityksellä on toimintaa Amerikassa ja sinne pitäisi saada palkattua kyberturvallisuusasiantuntija. Eräs tämän vähemmän tärkeäksi valinnut panelisti sanoikin henkilöstöresursseista, että "onkohan ikinä riittäviä, mutta tämä ei tule olemaan päähuolenaiheita Suomessa".

Haastattelujen mukaan kaikissa panelistien yrityksissä tullaan kuitenkin lisäämään kyberturvallisuuden henkilöstöresursseja, koska nykyiset eivät riitä enää vuonna 2021. Lisäys toimeenpannaan joko ihan perinteisesti palkkaamalla uutta henkilöstöä tai sitten antamaan nykyisille työntekijöille enemmän kyberturvallisuuteen liittyviä tehtäviä ja vastuita. Näin ollen kyberturvallisuudesta huolehtimiseen käytetyt henkilötyötunnit tulevat lisääntymään suomalaisissa valmistavan teollisuuden yrityksessä seuraavan 4-5 vuoden aikana. Esimerkkinä eräs panelisti antoi palvelupäälliköiden ja teknologiasta ymmärtävien kouluttamisen ottamaan vastuuta myös kyberturvallisuusasioista, jolloin kyberturvallisuutta tuodaan enemmän osaksi kaikkea muuta toimintaa.

Kyberturvallisuuden resursseihin liittyvä kohta *oikeat työkalut kyberturvallisuuden hallinnassa* jakoi hieman panelistien mielipiteitä. Lopulta vain yksi asiantuntijoista nosti sen tärkeäksi suomalaisen valmistavan teollisuuden näkökulmasta vuonna 2021. Kolme panelisteista sen sijaan argumentoivat asiaa seuraavasti: "Kyllä työkaluja aina löytyy", "konseptit on rakennettu jo vahvoiksi tuohon mennessä" ja "asiana en pistäisi fokusta tähän". Kyberturvallisuuden työkaluja kaikilla panelisteilla oli jotain käytössä, mutta kenelläkään ei tuntunut kuitenkaan olevan käytössä kokonaisvaltaista ja kaiken kattavaa työkalua. Koettiin kuitenkin, että yksi keskitetty työkalu voisi helpottaa toimia, mutta vain jos sen implementoiminen on tehtävissä järkevästi.

## 4.7 Asiantuntijapaneelin näkemykset verrattuna kirjallisuuskatsaukseen

Asiantuntijapanelisteilla oli monia samoja näkemyksiä kuin kirjallisuudessa, mutta joitakin kirjallisuuskatsauksessa mainittuja asioita paneeli ei nostanut tärkeiksi suomalaisen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021. Lisäksi panelistit mainitsivat ensimmäisellä delfoi-kierroksella asioita, jotka eivät tulleet erityisesti esille kirjallisuuskatsauksessa eivätkä myöskään nousseet toisella kierroksella tärkeimmiksi. Ainoastaan muutama näistä nousi toisella kierroksella ristiriitaisten, mahdollisesti tärkeiden asioiden joukkoon.

Seuraavan sivun taulukossa 4.1 on esitettynä tutkimuksen mukaan Suomen valmistavan teollisuuden kyberturvallisuuteen vaikuttavat asiat, jaoteltuna Deloitten kyberturvallisuuden viitekehyksen (*Cyber Security Framework*) [61, 62, 63] mukaisesti Strategisesti (*Strategic*), Turvallisesti (*Secure*), Valppaasti (*Vigilant*) ja Kestävästi (*Resilient*) -osa-alueiden alle. Kirjallisuuskatsauksessa luotuun taulukkoon 2.1 verrattuna tässä taulukossa on mukana myös delfoi-kierroksien aikana esille tulleet tärkeät asiat, joista toki vain osaa paneeli piti tärkeinä ja loppuja vähemmän tärkeinä tai mahdollisesti tärkeinä.

On huomattava, että taulukko 4.1 on tulevaisuuden suuntaa antava eikä absoluuttinen totuus - voi olla, että asiantuntijat jättivät jotain heikompia trendejä huomioimatta, jotka kirjallisuus taas on huomioinut vahvasti tai toisin päin. Myös kaikissa kohdissa kirjallisuuskatsauksessa ei ollut kyse valmistavasta teollisuudesta tai ainakaan suomalaisesta sellaisesta. Tällöin paneelin mielipide saattaa reflektoida juuri Suomen valmistavan teollisuuden näkökulmaa paremmin.

Lisäksi on huomioitava, että delfoi on menetelmänä haasteellinen heikkojen trendien ennakoinnissa. Delfoin yksimielisyyttä etsivien ominaisuuksien takia heikot trendit eivät aina tule esille, vaikka ne voisivat olla kiinnostaviakin. Myös tässä tutkimuksessa osa trendeistä saattaa olla jäänyt huomaamatta isompien ja ilmeisempien trendien hallitessa keskustelua. Suurimmilta osin heikompia trendejä on kuitenkin tässä työssä käsitelty luvussa 4.5.4 Muuta mahdollisesti tärkeää.

***Taulukko 4.1*** *Suomen valmistavan teollisuuden kyberturvallisuuteen vuonna 2021 vaikuttavia asioita - asiantuntijoiden näkemys vs. kirjallisuuskatsaus.*

| | **STRATEGISESTI** (STRATEGIC) | **TURVALLISESTI** (SECURE) | **VALPPAASTI** (VIGILANT) | **KESTÄVÄSTI** (RESILIENT) |
|---|---|---|---|---|
| **Tärkeää myös kirjallisuus-katsauksessa** | Esineiden internet eli IoT, Digitalisaatio ja "industry 4.0" | Teollisuus-automaation (ICS) turvallisuus, Saatavuuden varmistaminen, Identiteettien ja pääsynhallinta | | |
| **Mahdollisesti tärkeää, myös kirjallisuus-katsauksessa** | Käytettävyys vs. tietoturva, Vaatimusten, lakien ja asetuksien täyttäminen ja muutokset; Työntekijöiden kyberturvatietoisuus, Eri maiden erilaiset lait | Vastuiden määritys toimittajien ja muiden kumppanien kanssa, Pilviturvallisuus, Yksityisyydensuoja / tietosuoja, Mobiililaitteet, Vanhat teollisuus-automaatio-järjestelmät ja IT-ympäristöt, Kiristys ja terrorismi | Nollapäivä-haavoittuvuuksien hyödyntäminen, Edistyneet /kohdistetut kyberhyökkäykset (APT, Advanced Persistent Threats), Sisäpiiriuhkat, Automaation ja analytiikan lisääntyvä käyttö kyberturvallisuuden parantamisessa, Huijaukset | Kybervakoilu (myös valtiollisten toimijoiden tekemä), Kyberhyökkäyksiin varautuminen ja niistä toipuminen |
| **Mahdollisesti tärkeää, ei kirjallisuus-katsauksessa** | Koko organisaation kattavien toimintatapojen ja vision toteutus, Ympäristön kokonaiskuvan puuttuminen | Datan säilytys organisoidusti, Järjestelmien kompleksisuus ja monimuotoisuus | Oikeat työkalut kyberturvallisuuden hallintaan | Nopeat poliittiset muutokset ja muutokset toiminta-ympäristössä, Kyberturvaviestintä |
| **Vain kirjallisuus-katsauksessa, ei erityisesti panelisteilta** | Nuorten työntekijöiden sitouttaminen kyberturvalliseen kulttuuriin, Kasvavat reaaliaika- ja suorituskyky-vaatimukset | IoT ransomwaren suosion kasvu, Robotiikan turvallisuus, Muutoksien ja päivityksien hallinta, Kasvien datamäärien hallinta | Hyökkääjien ja hyökkäyksien tunnistaminen, Tietoturvan monitorointi-järjestelmät | |
| **Vähemmän tärkeä, mutta kirjallisuus-katsauksessa** | Tietoturvaosaajien puute, Kyberturvallisuus-resurssien puute ja kohdistaminen | | | |
| **Vähemmän tärkeä, ei kirjallisuus-katsauksessa** | Ylimmän johdon sitouttaminen, Viranomais-yhteistyön haasteet | | Kyberturvallisuuden mittaaminen | Maineriskien hallinta |

Taulukon 4.1 perusteella on kuitenkin mahdollista antaa yleistyksiä tärkeimmistä suuntaviivoista Suomalaisen valmistavan teollisuuden kyberturvallisuudesta vuonna 2021. Esimerkiksi sekä kirjallisuus että asiantuntijapaneeli sanoivat Strategisesti-puolen *IoT:n, digitalisaation ja industry 4.0:n* olevan tärkeää Suomen valmistavan teollisuuden kyberturvallisuudelle 2021.

Myös Turvallisesti-puolelle kirjallisuuskatsauksesta nousi selviä tärkeitä asioita, joita myös paneeli piti tärkeinä Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuudelle. Nämä tärkeät asiat olivat *saatavuuden varmistaminen, identiteetin ja pääsynhallinta* sekä *teollisuusautomaation (ICS) turvallisuus*. Kuitenkin mahdollisesti tärkeitä asioita, jotka sekä paneeli että kirjallisuuskatsaus toivat esille, oli Turvallisesti- ja Strategisesti-puolien lisäksi paljon esimerkiksi Valppaasti-alueella. Näistä hyvä esimerkki on erityisesti kirjallisuuden nostama analytiikan lisääntyvä käyttö kyberturvallisuuden parantamisessa.

Kirjallisuuskatsauksessa ilmeni muutama Strategisesti-puolen asia, joita paneeli ei kuitenkaan maininnut ollenkaan tai piti vähemmän tärkeinä Suomen valmistavan teollisuuden kyberturvallisuuden näkökulmasta vuonna 2021. Tässä voidaan nähdä hyvin paneelin positiivinen suhtautuminen kyberturvallisuuden tulevaisuuteen Suomessa, sillä esimerkiksi kirjallisuudessa vakavina kyberturvallisuuden tulevaisuuden uhkina nähdyt *tietoturvaosaajien puute* ja *nuorten työntekijöiden sitouttaminen kyberturvalliseen kulttuuriin* eivät erityisesti huolestuttaneet panelisteja.

Paneeli ei myöskään nostanut keskusteluun tai tuntunut kokevan erityisiä paineita kirjallisuudessa tulevaisuuden ongelmaksi mainitusta *kasvavista reaaliaika- tai suoritusvaatimuksista*. Vaikka panelistit myönsivät, että kiireessä liiketoiminta saattaa unohtaa kyberturvallisuuden, tuntui heillä silti olevan luotto siihen, että kukaan työntekijä ei lähtökohtaisesti halua vastustaa kyberturvallisuutta - kunhan vain kyberturvallinen toiminta on tehty heille tarpeeksi helpoksi.

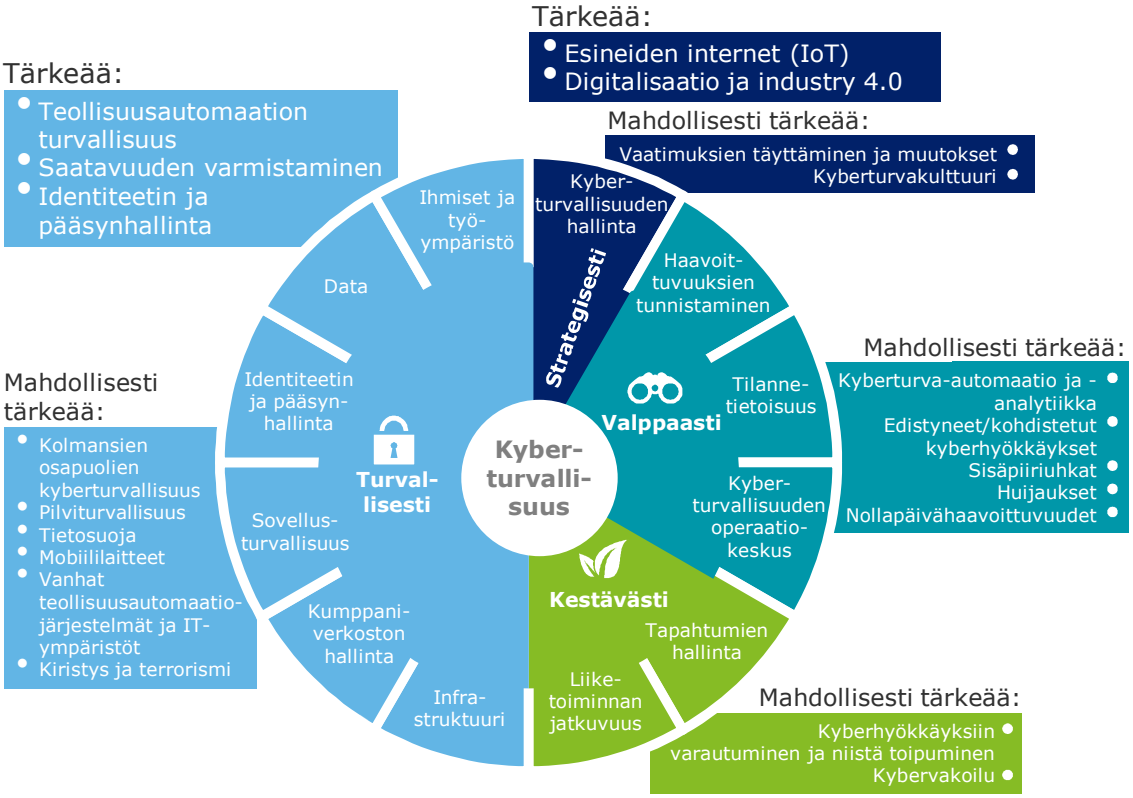
Kiinnostavaa oli myös, että vaikka paneeli sijoitti *identiteettien ja pääsynhallinnan* tärkeisiin asioihin, niin sen sijaan *identiteettivarkauksia*, jotka kuitenkin mainitaan kirjallisuudessa [11] valmistavankin teollisuuden ongelmaksi, ei kukaan ollut valinnut tärkeäksi Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021. Lisäksi vaikka *identiteettivarkaudet* tulivat myös esille ensimmäisellä kierroksella, niin yksi panelisteista koki sen jopa kuuluvan vähemmän tärkeiden asioiden joukkoon.

Yksi Kestävästi-osa-alueen mielenkiintoinen kohta taulukossa 4.1 on *kybervakoilu*,

jota kukaan panelisteista ei nostanut erityisesti tärkeäksi, mutta ei myöskään vähemmän tärkeäksi asiaksi. Kirjallisuudessa kybervakoilusta oli huomattavasti enemmän puhetta, mutta tutkimuksen perusteella se vaikuttaa koskevan vielä kuitenkin vakavammin ulkomaisia kuin kotimaisia yrityksiä. Tästä huolimatta, kybervakoilu nostetaan esille Suomen suojelupoliisin uusimmassa, vuonna 2017 julkaistussa vuosikirjassa: "Tuotekehitystä tekeviin yrityksiin kohdistuva vieraiden valtioiden oikeudeton tiedonhankinta sekä kriittiseen infrastruktuuriin kohdistuvat verkkouhat eivät ole ilmiöinä kadonneet." Kybervakoilusta Suomessa Supo sanoo, että "tieteellis-tekninen tiedustelu keskittyy huipputekniikkaan ja sen sovelluksiin. Suomessa keskeisiä kiinnostuksen kohteita ovat elektroniikka-, laiva- ja energiateollisuus." [92]. Näin ollen voidaan ehkä todeta, että tämä kybervakoilu on yksi niistä heikommista trendeistä, jotka eivät delfoi-kierrosten jälkeen erityisesti tulleet esille, mutta jotka silti mahdollisesti vaikuttavat Suomen valmistavan teollisuuden kyberturvallisuustoimiin seuraavien 4-5 vuoden aikana.

# 5. YHTEENVETO

Kuvassa 5.1 on tämän delfoi-tutkimuksen tärkeimmät tulokset jaoteltuina luvussa 2.5 esitellyn Deloitten kyberturvallisuuden viitekehyksen mukaisesti.




***Kuva 5.1*** *Delfoi tutkimuksen tulosten yhteenveto jaoteltuna Deloitten kyberturvallisuuden viitekehyksen mukaisesti.*

Kuten kuvasta 5.1 näkee, tämän tutkimuksen mukaan Suomen valmistavan teollisuuden kyberturvallisuuteen vuonna 2021 eniten vaikuttavia asioita ovat todennäköisesti IoT, digitalisaatio, industry 4.0 ja teollisuusautomaation turvallisuus. Myös identiteetin ja pääsynhallinta sekä saatavuuden varmistaminen tulevat olemaan tär-

keitä.

Lisäksi tutkimuksessa ilmeni joukko asioita, joiden tärkeys Suomen valmistavan teollisuuden kyberturvallisuudelle vuonna 2021 ei ole yhtä selvä kuin edellisten. Asiat on luokiteltu tässä tutkimuksessa sekä kuvassa 5.1 mahdollisesti tärkeiksi, ja niiden tärkeyttä on tarkasteltava vielä tarkemmin jatkotutkimuksissa.

Vastaavasti vähemmän tärkeitä asioita, joihin Suomen valmistava teollisuus tuskin tulee vuonna 2021 enää panostamaan niin paljon, ovat ainakin ylimmän johdon sitouttaminen, maineriskien hallinta, viranomaisyhteistyön haasteet ja kyberturvallisuuden mittaaminen. Monien näistä asioista katsotaan olevan jo kunnossa vuonna 2021, jolloin niitä tarvitsee lähinnä vain ylläpitää. Näin ollen kyberturvallisuuden resurssit sekä investoinnit voidaan suunnata jo muualle.

Kuten yleensä muuhunkin liiketoimintaan, niin myös onnistuneeseen kyberturvallisuuden hallintaan kuuluu suunnitelmallisuus ja resurssien oikea-aikainen kohdistaminen. Tämä tutkimuksen tarkoitus oli auttaa Suomen valmistavan teollisuuden kyberturvallisuuden kanssa työskenteleviä arvottamaan, priorisoimaan ja suunnittelemaan paremmin työtehtäviään, investointejaan sekä rajallisten resurssiensa käyttöä. Tällöin heillä on mahdollisuus proaktiivisesti varautua tulevaisuuden kyberturvallisuushaasteisiin ja kehittää kyberturvallisuuden hallintaa kohti reaaliaikaisuutta. Tutkimus auttaa myös Deloitten Cyber Risk -tiimiä ymmärtämään ja tukemaan entistä paremmin kyseisen toimialan asiakkaitaan.

Vaikka tutkimuksen laajuuden puitteissa ei jokaiseen esille tuotuun lähitulevaisuuden kyberturvallisuushaasteeseen voitu esittää ratkaisua tai tarkkaa ennustetta, tutkimus kuitenkin auttaa kyberturvallisuuden ammattilaisia ymmärtämään paremmin Suomen valmistavan teollisuuden tulevaisuuden jatkuvasti muuttuvaa, monimuotoista ja laajaa kybertoimintaympäristöä. Muutamia kirjallisuuden esittämiä toimenpidesuosituksia valmistavan teollisuuden kyberturvallisuuden parantamiseksi on kuitenkin poimittu tämän työn liitteeseen 6.

## 5.1 Työn onnistumisen arviointi

Tämä työ voidaan kokonaisuutena katsoa onnistuneeksi, sillä se antoi vastauksia asetettuihin tutkimuskysymyksiin. Tästä huolimatta prosessin aikana eteen tuli myös haasteita, joita tässä luvussa käsitellään tarkemmin.

Tutkimuksen tuloksien reflektointi ja arviointi on myös Kuusen [29] mukaan osa delfoi-tutkimuksen raportointia. Kuusi ehdottaa arvioinnin perustaksi esimerkiksi seuraavaa kuutta menetelmän menestyneen käytön ehtoa:

1. onnistuminen asiantuntijapaneelin valinnassa,
2. anonyymi argumentointi, joka ei ole pelkästään asiantuntijoiden perustelemattomien mielipiteiden esittämistä vaan yhä enenevässä määrin keskittyy faktuaalisten argumenttien esittämiseen keskustelun kohteena olevista kysymyksistä,
3. onnistuminen mielekkäiden kysymystenasettelujen (eli topicien) etsimisessä,
4. stukturoitu keskustelu, jossa jatkuvasti ja systemaattisesti arvioidaan esitettyjen topicien ja niitä kommentoivien argumenttien pätevyyttä (arviointia tulee tulevaisuusväitteiden tai skenaarioiden osalta tehdä paitsi niiden toteutumisesta myös mm. tärkeydestä, toivottavuudesta ja toteutumisen erilaisista esteistä tai edellytyksistä);
5. kyky koota systemaattisesti arvioiden, kasautuvasti ja käyttäjäystävällisesti relevantteja tulevaisuusargumentteja monilta ja monenlaisilta asiantuntijoilta, ja
6. tuotetun aineiston relevanssi strategisen päätöksenteon kannalta.

Asiantuntijapaneelin valinta oli tutkimuksen tavoitteiden näkökulmasta onnistunut, sillä panelistien taustat olivat riittävän vaihtelevia ja asiantuntijat alan kokeneita ammattilaisia. Toki koska kyseessä on hyvin erilaisista yrityksistä koostuva Suomen valmistava teollisuus, olisi suurempi paneeli voinut esittää enemmän näkemyksiä ja laajemman näkökulman alan kyberturvallisuuden tulevaisuudesta. Suuremman paneelin kokoaminen olisi kuitenkin vaatinut enemmän resursseja kuin tähän tutkimukseen oli käytettävissä. Oma haasteensa oli myös tavoittaa sopiviksi tunnistetut henkilöt paneeliin sekä saada sovittua tapaamiset delfoi-kierroksien haastatteluja varten. Tämä vei arvioitua enemmän aikaa ja viivästytti hieman tutkimuksen alkua, kuten myös tutkimuksen alkupäähän sattuneet joululomat ja vuoden vaihtuminen.

Anonyymi argumentointi onnistui delfoi-kierroksien aikana hyvin. Asiantuntijoilla oli yleensä hyvät perustelut omille näkemyksilleen ja ne perustuivat tosiasioihin, joista panelisteilla oli yleisesti hyvä näkemys ammattinsa puolesta. Delfoi-kierroksien

haastattelutilanteissa haastavaa oli saada asiantuntijapanelistit keskittymään nimenomaan tulevaisuuteen, kun keskustelujen aikamuoto helposti kääntyi menneeseen tai tähän hetkeen. Toisella delfoi-kierroksella tähän kuitenkin kiinnitettiin enemmän huomiota esimerkiksi tarkemmilla kysymysasetteluilla, ja näin keskustelu pysyi ensimmäistä kierrosta paremmin tulevaisuusorientoituneena.

Yleisesti kysymysten asettelu onnistui hyvin erityisesti toisella kierroksella. Ensimmäisen delfoi-kierroksen kysymyksistä osa huomattiin tutkimuksen edetessä tarpeettomiksi tai heikommin muotoilluiksi, mutta niiden tarkentaminen ja tiettyihin teemoihin ja asioihin keskittyminen toisella kierroksella auttoi lopulta saamaan paneelilta tutkimuksen tavoitteita ajatellen tärkeimmät asiat esille.

Keskustelun strukturointi ja esimerkiksi ajankäyttö paranivat myös toisella kierroksella. Ensimmäisellä kierroksella joidenkin haastattelujen lopussa tuli hieman kiire, mutta toisella kierroksella tunnin aika riitti hyvin. Tähän toki auttoi myös se, että ensimmäisen kierroksen jälkeen panelistien vastaustyylit olivat jo tuttuja. Myös PowerPoint-esityksen käyttö tuki toisen kierroksen haastatteluja: kun esityksessä vaihtoi kalvosta toiseen, samalla myös aiheen vaihto sujui nopeammin eikä yhteen aiheeseen kulutettu liikaa aikaa.

Näistä haasteista huolimatta ensimmäinen delfoi-kierros kuitenkin onnistui tärkeimmässä tavoitteessaan eli valmistavan teollisuuden kyberturvallisuuden tulevaisuudelle relevanttien aiheiden kokoamisessa seuraavalle kierrokselle. Lisäksi ensimmäiseltä kierrokselta nousi paljon hyviä väittämiä, joista mielenkiintoisimpien valitseminen toiselle kierrokselle oli oma haasteensa. Tämä ratkaistiin jaottelemalla väittämät mitä, miksi ja miten -otsikoiden alle, jolloin näiden ulkopuolella olevat väittämät oli mahdollista karsia pois.

Molemmilla kierroksilla keskustelu oli hyvää myös siksi, että panelistin esittämien argumenttien tueksi oli mahdollista saman tien kysyä perusteluja. Tämä todennäköisesti vähensi väärinymmärryksien riskiä. Lisäksi muiden panelistien esittämiä väittämiä saattoi reflektoida muiden panelistien haastatteluissa ja väittämien pätevyyttä pystyi tarkastamaan toisilta panelisteilta heidän haastatteluidensa aikana. Panelistit eivät myöskään arvioineet vain tiettyjen väittämien tai asioiden toteutumisen todennäköisyyttä, vaan myös esimerkiksi tietyn asian merkittävyydestä ja toivottavuudesta panelistit antoivat argumenttejaan ja reflektoivat toistensa mielipiteitä. Lisäksi keskustelua syntyi tiettyjen asioiden toteutumisen edellytyksistä ja esteistä, mikä auttoi argumenttien ja väittämien pätevyyden arvioinnissa.

Tutkimuksen tuloksien analyysissä suurimpana haasteena oli yhdistellä yksittäisistä kommenteista eri asioita eri kohdista eri henkilöiden haastatteluja, sekä osata erityisesti ensimmäisellä kierroksella tulkita, mitä asiantuntija mahdollisesti tarkoitti esimerkiksi sanoessaan tietyn asian useamman kerran haastattelujen aikana. Haastavuudestaan huolimatta näiden asioiden analysoiminen oli kuitenkin ensimmäisellä delfoi-kierroksella erityisen tärkeää, jotta toisen kierroksen keskusteluihin saatiin tuotua oikeat asiat.

Listan viimeinen kohta "tuotetun aineiston relevanssi strategisen päätöksenteon kannalta" on varmasti riippuvainen yrityksestä, mutta ainakin asiantuntijapaneelin jäsenien ja heidän yrityksiensä näkökulmasta tässä tutkimuksessa tuodaan vertailupohjaa muilta Suomen valmistavan teollisuuden yrityksiltä, mikä helpottaa muun muassa tulevaisuuden kyberturvallisuuden resurssienkäytön suunnittelua sekä toimialan kokonaiskuvan hahmottamista. Aineistoa on myös mahdollisuus käyttää pohjana keskustelulle koko organisaation tasolla. Suomen valmistavanteollisuuden kyberturvallisuuden ammattilainen voi käyttää yksityiskohtia tai yleistyksiä tästä tutkimuksesta omien argumenttiensa tukena esimerkiksi investointikeskusteluja käytäessä.

Deloitten strategisessa päätöksenteossa tätä tutkimusta on mahdollista käyttää pohjana esimerkiksi tulevaisuuden tarjooman suunnittelussa ja kehittämisessä: mitkä asiat kyberturvallisuudelle kiinnostavat suomalaisen valmistavan teollisuuden asiakkaita ja millaisia tavoitteita heillä on kyberturvallisuuteensa suhteen. Tutkimus auttaa Deloittea myös tulevaisuudessa vastamaan näihin asiakkaidensa tarpeisiin ja tarjoamaan heitä kyberturvallisuustyössään tukevia palveluita. Tämä on tärkeää, jotta Deloitte voi tulevaisuudessakin toimia asiakkaidensa strategisena kyberturvallisuusneuvonantajana ja -kumppanina. Näin Deloitte voi auttaa asiakkaitaan nostamaan kyberturvallisuutensa strategiselle tasolle, missä kyberturvallisuuden hallinta on reaktiivisen sijaan proaktiivista.

Toisen kierroksen haastattelujen jälkeen tuloksia analysoitaessa ilmeni myös, että joihinkin asioihin ja kohtiin työssä olisi kolmas haastattelukierros voinut tuoda syvemmän ymmärryksen ja enemmän näkökulmia. Työn laajuuden puitteissa kolmas kierros ei kuitenkaan ollut mahdollinen. Tästä syystä jotkin kohdat tutkimuksessa saattoivat jäädä osittain pintapuolisiksi ja niitä tulee tutkia vielä tarkemmin. Nämä jatkotutkimustarpeet on käsitelty tarkemmin seuraavassa luvussa.

## 5.2 Jatkotutkimustarpeet

Koska tutkimuksen aihe on laaja ja siitä ei viime aikoina olla tehty merkittävää tieteellistä tutkimusta, jää tämän tutkimuksen jälkeen tarpeita jatkotutkimukselle. Niistä tärkeimmät on esitelty alla. Pidempi lista ehdotuksia jatkotutkimuksien tutkimuskysymyksiksi on koottu liitteeseen 7.

Jatkossa tätä tutkimusta on mahdollista jatkaa pidemmälle aikavälille kuin ainoastaan vuoteen 2021. Myös vuonna 2021 voi olla mielenkiintoista tutkia, toteutuivatko tutkimuksessa annetut ennusteet ja miksi. Tämä saattaa taas helpottaa sen hetkistä tulevaisuuden ennakointia. Tutkimusta on myös mahdollista leventää useampaan yritykseen tai jopa toimialaan. Tällöin eri toimialojen tilanteiden vertaaminen saattaa olla mielekästä.

Lisäksi tutkimuksesta ilmenneisiin eri teemoihin olisi jatkossa syytä paneutua tarkemmin. Tärkeää olisi tutkia enemmän esimerkiksi sitä, näkeekö Suomen valmistava teollisuus kyberturvallisuuteen panostamisen tulevaisuudessakin lähinnä vain kustannuksena vai osataanko se nähdä myös investointina - ja olisiko tätä asennetta mahdollista muuttaa. Tämän tutkimuksen mukaan Suomen valmistava teollisuus näkee melko yleisesti kyberturvallisuuden kustannuksena, eikä tähän kehityssuuntaan välttämättä ole nähtävissä muutosta seuraavan viiden vuoden aikana. Myös valmistavan teollisuuden tulevaisuuden kyberturvallisuuden investointiaikeita on tutkittava vielä enemmän.

Selvimmät jatkotutkimustarpeet koskevat tässä tutkimuksessa mahdollisesti tärkeiksi tunnistettuja Suomen valmistavan teollisuuden kyberturvallisuuteen vuonna 2021 vaikuttavia asioita. Tämän tutkimuksen pohjalta ei voida vielä tarpeeksi hyvin ennakoida, mikä näiden asioiden merkitys ja todennäköisyys on tulevaisuudessa. Näitä asioita ilmeni tutkimuksessa pitkä lista, joista jokaista on syytä tutkia vielä syvemmin.

Edellisten lisäksi jatkossa on analysoitava vielä tarkemmin kyberturvallisuuden määritelmää ja siten kartoittaa valmistavan teollisuuden kuin muidenkin toimialojen käsityksiä siitä. Myös Suomen valmistavan teollisuuden kyberturvallisuuden tavoitteita ja niiden saavuttamiseksi tehtyjä suunnitelmia saattaisi olla mielenkiintoista vertailla ja tutkia vielä syvällisemmin.

# LÄHTEET

[1] *Deloitte Cybersecurity Framework*, Deloitte Cyber Risk, 2017, rajoitettu saatavuus.

[2] *Suomen kyberturvallisuusstrategia ja taustamuistio*, Turvallisuuskomitean sihteeristö, 2013, 44 s. .Saatavissa (viitattu 24.5.2017): http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia.

[3] M. Lehto and A. Kähkönen, *Kyberturvallisuuden kansallinen osaaminen*, Jyväskylän yliopisto, 2015, Saatavissa (viitattu 24.5.2017): https://www.jyu.fi/it/tutkimus/202015_Kyber_kansallinen_osaaminen_VERKKO.pdf.

[4] *Nelikenttäanalyysi - SWOT*, Suomen riskienhallintayhdistys, 2013, Saatavissa (viitattu 24.5.2017): http://www.pk-rh.fi/index.php?page=swot.

[5] M. Lehto, J. Limnéll, E. Innola, J. Pöyhönen, T. Rusi, and M. Salminen, *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi*, Valtionneuvoston kansliasivistys- ja tutkimustoiminta, 2017, 79 s. Saatavissa (viitattu 24.5.2017): http://tietokayttoon.fi/julkaisu?pubid=17805.

[6] *Verizon 2017 Data Breach Investigations Report*, Verizon, 2017, 76 s. Saatavissa (viitattu 24.5.2017): http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

[7] *Verizon 2016 Data Breach Investigations Report*, Verizon, 2016, 85 s. Saatavissa (viitattu 24.5.2017): http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[8] *Renault stops production at some sites after cyber attack*, Daily Mail, MailOnline, 2017, Saatavissa (viitattu 24.5.2017): http://www.dailymail.co.uk/wires/reuters/article-4502266/Renault-stops-production-sites-cyber-attack.html.

[9] *2016 Cyber Security Intelligence Index*, IBM X-Force, 2016, Saatavissa (viitattu 24.5.2017): http://www-03.ibm.com/security/data-breach/cyber-security-index.html.

[10] *2017 Cyber Security Intelligence Index*, IBM X-Force, 2017, Saatavissa (viitattu 24.5.2017): https://www-03.ibm.com/security/data-breach/threat-intelligence-index.html.

[11] *2017 Internet Security Threat Report*, Symantec, 2017, 77 s. Saatavissa (viitattu 24.5.2017): https://www.symantec.com/security-center/threat-report.

[12] *Threat Horizon 2019: Disruption. Distortion. Deterioration.*, Information Security Forum, 2017, 56 s. Rajoitettu saatavuus: https://www.isflive.org/docs/DOC-22025/.

[13] *AT&T Cybersecurity Insights: What Every CEO Needs to Know About Cybersecurity - Decoding the Adversary*, AT&T, 2015, 36 s. Saatavissa (viitattu 24.5.2017): https://www.business.att.com/cybersecurity/docs/decodingtheadversary.pdf.

[14] *Tech Trends 2017: The kinetic enterprise*, Deloitte University, 2017, 136 s. Saatavissa (viitattu 24.5.2017): https://www2.deloitte.com/us/en/pages/technology/articles/technology-consulting-tech-trends-collection.html.

[15] *EMEA 360 Boardroom Survey*, Deloitte, 2016, 40 s. Saatavissa (viitattu 24.5.2017): http://www2.deloitte.com/uk/en/pages/finance/articles/emea-360-boardroom-survey.html.

[16] *Navigating legacy: Charting the course to business value - 2016–2017 global CIO survey*, Deloitte University, 2016, 68 s. Saatavissa (viitattu 24.5.2017): https://dupress.deloitte.com/content/dam/dup-us-en/articles/3591_2016-2017-CIO-survey/DUP_2016-2017-CIO-survey.pdf.

[17] *Information Risk Assessment Methodology 2 (IRAM2)*, Information Security Forum, 2017, Saatavissa (viitattu 24.5.2017): https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/.

[18] *Cost of Data Breach Study*, IBM Security: Ponemon Institute, 2016, Saatavissa (viitattu 24.5.2017): http://www-03.ibm.com/security/data-breach/.

[19] *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, 2016, 31 s. .Saatavissa (viitattu 24.5.2017): http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=BUL12370USEN&attachment=BUL12370USEN.PDF.

[20] E. Mossburg, H. Calzada, and J. Gelinne, *Beneath the surface of a cyberattack A deeper look at business impacts*, 2016, 25 s. Saatavissa (viitattu 24.5.2017): https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-global-risk-advisory-report-beneath-the-surface-of-a-cyberat....pdf.

[21] J. Tapanainen, *Valmistavan teollisuuden evoluutio ja revoluutio*, Tieto Oyj, 2016, Saatavissa (viitattu 24.5.2017): https://www.tieto.fi/nakemyksia-ja-visioita/valmistavan-teollisuuden-evoluutio-ja-revoluutio.

[22] *Industry 4.0: An Introduction*, Deloitte, 2015, Saatavissa (viitattu 24.5.2017): http://www2.deloitte.com/be/en/pages/operations/articles/Industry_40.html.

[23] J. Paasi and N. Wessberg, *Menestyvää liiketoimintaa suomalaisissa valmistavan teollisuuden yrityksissä 2020-luvulla – Neljä skenaariota*, VTT, 2016, 54 s. Saatavissa (viitattu 24.5.2017): http://www.vtt.fi/inf/pdf/visions/2016/V8.pdf.

[24] *Pictures of the Future*, Siemens, 2016, Saatavissa (viitattu 24.5.2017): https://www.siemens.com/innovation/en/home/pictures-of-the-future.html.

[25] M. Tyynelä, *Tietoturvan merkitys on korostunut teollisuusautomaation ylläpidossa*, Promaint, 2015, Saatavissa (viitattu 24.5.2017): http://www.promaintlehti.fi/Turvallisuus-ja-ymparisto/Tietoturvan-merkitys-on-korostunut-teollisuusautomaation-yllapidossa.

[26] *Talouselämä 500*, Talouselämä, 2016, Saatavissa (viitattu 1.2.2016): http://www.talouselama.fi/uutiset/talouselama-21-2016-talouselama-500-suomen-suurimmat-yritykset-6554669.

[27] *Tuloksentekijät 2016*, Kauppalehti, 2016, Saatavissa (viitattu 1.2.2017): http://www.kauppalehti.fi/5/i/yritykset/menestyjat/lista.jsp?id=3&maakunta=0&kunta=0&toimiala=0&sivu=1&sortby=v1&sort=desc.

[28] *Delfoi-metodi*, eDelfoi, 2012, Saatavissa (viitattu 24.5.2017): https://edelfoi.fi/viewbulletin.page?bulletinId=5.

[29] O. Kuusi, *Delfoi-menetelmä*, Metodix, 1999, Saatavissa (viitattu 24.5.2017): https://metodix.net/2014/05/19/kuusi-delfoi-metodi/.

[30] R. Popper, *How are foresight methods selected?*, Foresight, 2008, ss. 62-89, 27 s. Saatavissa (viitattu 24.5.2017): http://www.emeraldinsight.com/doi/abs/10.1108/14636680810918586.

[31] C. Okoli and S. D. Pawlowski, *The Delphi Method as a Research Tool: An Example, Design Considerations and Applications*, Information & Management, 2003, 20 s. Saatavissa (viitattu 24.5.2017): http://www.sciencedirect.com/science/article/pii/S0378720603001794.

[32] V. Valtonen, *Turvallisuustoimijoiden yhteistyö operatiivistaktisesta näkökulmasta*, Maanpuolustuskorkeakoulu, Taktiikan laitos, 2010, 299 s. Saatavissa (viitattu 24.5.2017): https://www.doria.fi/bitstream/handle/10024/74154/Valtonen%2B-%2BTurvallisuustoimijoiden%2Byhteistyo.pdf?sequence=1.

[33] M. Makkonen, S. Pätäri, A. Jantunen, and S. Viljainen, *Competition in the European electricity markets – outcomes of a Delphi study*, LUT Energy, Laboratory of Electricity Markets and Power Systems, Lappeenranta University of Technology, 2012, energy Policy, ss. 431–440, 10 s. Saatavissa (viitattu 24.5.2017): http://www.sciencedirect.com.libproxy.tut.fi/science/article/pii/S0301421512001309.

[34] *Kyberturvallisuus digitalisoituvassa maailmassa*, CGI, 2016, Saatavissa (viitattu 24.5.2017): http://www.cgi.fi/tietoturva/lataa-white-paper.

[35] *Kyberturvallisuuskeskuksen vuosiraportti 2015*, Viestintäviraston Kyberturvallisuuskeskus, 2016, 25 s. Saatavissa (viitattu 24.5.2017): https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2016/kyberturvallisuuskeskuksenvuosikatsaus2015.html.

[36] *Tietoturvan vuosi 2016*, Viestintävirasto, 2017, 13 s. Saatavissa (viitattu 24.5.2017): https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2017/tietoturvanvuosi2016.html.

[37] M. Sundquist *et al.*, *Teollisuusautomaation tietoturva: Verkottumisen riskit ja niiden hallinta*, Suomen Automaatioseura ry, 2010, 160 s. Verkkopainos Saatavissa (viitattu 24.5.2017): https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf.

[38] *ENISA Threat Landscape 2016*, ENISA, 2017, 86 s. Saatavissa (viitattu 24.5.2017): https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

[39] *ENISA Threat Landscape 2015*, ENISA, 2016, 88 s. Saatavissa (viitattu 24.5.2017): https://www.enisa.europa.eu/publications/etl2015.

[40] *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*, ENISA, 2015, 40 s. Saatavissa (viitattu 24.5.2017): https://www.enisa.europa.eu/publications/maturity-levels.

[41] *Internet Organised Crime Threat Assessment (IOCTA) 2016*, Europol's European Cybercrime Centre (EC3), 2016, 72 s. Saatavissa (viitattu 24.5.2017): https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

[42] *AT&T Cybersecurity Insights: The CEO's Guide to Securing the Internet of Things*, AT&T, 2016, 24 s. Saatavissa (viitattu 24.5.2017): https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf.

[43] L. Kessem, *Ransomware: How consumers and businesses value their data*, IBM X-Force Research, 2016, 23 s. Saatavissa (viitattu 24.5.2017): https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03135USEN&.

[44] *Kaspersky Security Bulletin: Ppedictions for 2017'Indicators of Compromise' are Dead*, Kaspersky Lab, 2016, 21 s. Saatavissa (viitattu 24.5.2017): https://securelist.com/analysis/kaspersky-security-bulletin/76660/kaspersky-security-bulletin-predictions-for-2017/.

[45] *The Global State of Information Security Survey 2016: Industrial products summary*, PwC - PricewaterhouseCoopers LLP, 2015, Saatavissa (viitattu 24.5.2017): http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/industry/industrial-products.html.

[46] *List of Cybersecurity Associations*, Cybersecurity Ventures, 2015, Saatavissa (viitattu 24.5.2017): http://cybersecurityventures.com/cybersecurity-associations/.

[47] *CISRE — The Center for Information Security Research and Education*, University of Houston, 2016, Saatavissa (viitattu 24.5.2017): http://uh.edu/tech/cisre/.

[48] *The Center for Education and Research in Information Assurance and Security (CERIAS)*, Purdue University, 2016, Saatavissa (viitattu 24.5.2017): https://www.cerias.purdue.edu/.

[49] *Digital Risk and Security*, Gartner, 2016, Saatavissa (viitattu 24.5.2017): http://www.gartner.com/technology/topics/digital-risk-security.jsp#.

[50] H. Shey *et al.*, *The Cybercriminal's Prize: Your Customer Data And Intellectual Property*, Forrester, 2015, 88 s. Saatavissa (viitattu 24.5.2017): https://www.forrester.com/report/The+Cybercriminals+Prize+Your+Customer+Data+And+Intellectual+Property/-/E-RES61544?objectid=RES61544.

[51] *Teollisuuden kyberturvallisuus*, VTT, 2015, Saatavissa (viitattu 24.5.2017): http://www.vtt.fi/teollisuuden-kyberturvallisuus.

[52] Pelkonen *et al.*, *Kyberosaaminen Suomessa*, Valtionneuvoston sivistys- ja tutkimustoiminta, 2016, 90 s. Saatavissa (viitattu 24.5.2017): http://tietokayttoon.fi/documents/10616/2009122/9_Kyberosaaminen+Suomessa.pdf/29c8f675-0790-4c2f-91c2-69187b34b37e?version=1.0.

[53] *Dyn Statement on 10/21/2016 DDos Attack*, Dyn, 2016, Saatavissa (viitattu 24.5.2017): http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/.

[54] *Erikoisraportti: Suojaamattomien automaatiolaitteiden kartoitus 2016*, Viestintävirasto, 2016, 11 s. Saatavissa (viitattu 24.5.2017): https://www.viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Erityisraportti_Suojaamattomia_automaatiolaitteita_suomalaisissa_verkoissa_2016.pdf.

[55] *Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*, Turvallisuuskomitea, 2014, 60 s. .Saatavissa (viitattu 24.5.2017): http://turvallisuuskomitea.fi/index.php/files/18/muut%20julkaisut/11/Kyberturvallisuusstrategian%20toimeenpano-ohjelma.pdf.

[56] N. Ulltveit-Moe, H. Nergaard, L. Erdödi, T. Gjøsæter, E. Kolstad, and P. Berg, *Secure Information Sharing in an Industrial Internet of Things*, University of Agder, Norway, 2016, 12 s. Saatavissa (viitattu 24.5.2017): https://arxiv.org/pdf/1601.04301.pdf.

[57] T. Davenport and A. Amjad, *The future of cybersecurity*, Deloitte University, 2016, Saatavissa (viitattu 24.5.2017): http://dupress.deloitte.com/dup-us-en/topics/analytics/future-of-cybersecurity-in-analytics-automation.html#endnote-sup-1.

[58] R. Contu and E. Perkins, *How the Internet of Things Will Impact Cybersecurity*, Gartner, 2016, 9 s. Saatavissa (viitattu 24.5.2017): https://www.gartner.com/doc/3294329/internet-things-impact-cybersecurity.

[59] S. B. Alaybeyi, *Don't Be Misled by the IoT Security Myths*, Gartner, 2016, 10 s. Saatavissa (viitattu 24.5.2017): https://www.gartner.com/doc/3327223/dont-misled-iot-security-myths.

[60] *2017 Threats Predictions*, McAfee Labs, 2016, 57 s. Saatavissa (viitattu 24.5.2017): https://www.mcafee.com/au/resources/reports/rp-threats-predictions-2017.pdf.

[61] I. Saif, S. Peasley, and A. Perinkolam, *Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age*, Deloitte University Press, Deloitte Review, 2015, 19 s. Saatavissa (viitattu 24.5.2017): https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html.

[62] *RBI Guidelines for Cyber Security Framework*, Deloitte, 2016, 7 s. Saatavissa (viitattu 24.5.2017): https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-rbi-guidelines-for-cyber-security-framework-noexp.pdf.

[63] *Services: Cyber Risk*, Deloitte Global, 2017, Saatavissa (viitattu 24.5.2017): https://www2.deloitte.com/global/en/pages/risk/solutions/cyber-risk.html.

[64] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, *Security and Privacy Challenges in Industrial Internet of Things*, Technische Universität Darmstadt, Germany, 2015, 6 s. Saatavissa (viitattu 24.5.2017): http://ieeexplore.ieee.org/document/7167238/.

[65] S. Wang, J. Wan, D. Li, and C. Zhang, *Implementing Smart Factory of Industrie 4.0: An Outlook*, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, 2016, 10 s. Saatavissa (viitattu 24.5.2017): https://www.researchgate.net/publication/291385881_Implementing_Smart_Factory_of_Industrie_40_An_Outlook.

[66] *AT&T Cybersecurity Insights: The CEO's Guide to Data Security*, AT&T, 2017, 20 s. Saatavissa (viitattu 24.5.2017): https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf.

[67] A. Spadafora, *The average IoT device is compromised after being online for 6 minutes*, ITProPortal, 2016, Saatavissa (viitattu 24.5.2017): http://www.itproportal.com/news/the-average-iot-device-is-compromised-after-being-online-for-6-minutes/.

[68] *Will the Internet of Things be bigger than the Industrial Revolution?*, Business Insider Nordic, 2016, Saatavissa (viitattu 24.5.2017): http://nordic.businessinsider.com/will-the-internet-of-things-be-bigger-than-the-industrial-revolution-2016-9/.

[69] *'Internet of Things' Connected Devices to Triple by 2021, Reaching over 46 Billion Units*, Juniper Research, 2016, Saatavissa (viitattu 24.5.2017): https://www.juniperresearch.com/press/press-releases/'internet-of-things'-connected-devices-to-triple-b.

[70] I. Saif, S. Peasley, and A. Perinkolam, *Safeguarding the Internet of Things*, Deloitte University Press, 2016, 18 s. Saatavissa (viitattu 24.5.2017): https://www2.deloitte.com/gt/es/pages/risk/articles/safeguarding-the-internet-of-things.html.

[71] *Internet Of Things; A Vision For The Future*, OTA, Online Trust Alliance, 2016, 4 s. Saatavissa (viitattu 24.5.2017): https://otalliance.org/news-events/press-releases/ota-publishes-vision-future-internet-things.

[72] J. Lee *et al.*, *Introduction to cyber manufacturing*, Manufacturing Letters, Society of Manufacturing Engineers (SME), no. 8, ss.11-15, 5 s., University of Cincinnati, United States, 2016.

[73] *Global Information Security Workforce Study*, ISC2, 2017, Saatavissa (viitattu 24.5.2017): https://www.isc2.org/pressreleasedetails.aspx?id=14570.

[74] *Are Millennials the Latest Security Threat?*, Software Advice, 2015, Saatavissa (viitattu 24.5.2017): http://www.softwareadvice.com/security/industryview/millennial-threat-report-2015/.

[75] J. Fleming and A. Adkins, *Data Security: Not a Big Concern for Millennials*, Gallup, 2016, Saatavissa (viitattu 24.5.2017): http://www.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx.

[76] *Meet the Millenials - The Next Generation of Your Information Security Workforce*, Frost & Sullivan, 2017, Saatavissa (viitattu 24.5.2017): https://iamcybersafe.org/research_millennials/.

[77] *Millennials changing the face of cybersecurity*, SC Magazine US, 2016, Saatavissa (viitattu 24.5.2017): https://www.scmagazine.com/millennials-changing-the-face-of-cybersecurity/article/568981/.

[78] D. D. Caputo, S. L. Pfleeger, M. A. Sasse, P. Ammann, J. Offutt, and L. Deng, *Barriers to Usable Security? Three Organizational Case Studies*, the IEEE Computer and Reliability Societies, 2016, 11 s. Saatavissa (viitattu 24.5.2017): http://discovery.ucl.ac.uk/1530502/1/Caputo_Barriers%20to%20Usable%20Security_Three%20Organizational%20Case%20Studies.pdf.

[79] A. Beautement, I. Becker, S. Parkin, K. Krol, and M. A. Sasse, *Productive Security: A scalable methodology for analysing employee security behaviours*, University College London, USENIX Association, 2016, 19 s. Saatavissa (viitattu 24.5.2017): https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-beautement.pdf.

[80] E. Kovacs, *IBM Reports Significant Increase in ICS Attacks*, Securityweek, 2016, Saatavissa (viitattu 24.5.2017): http://www.securityweek.com/ibm-reports-significant-increase-ics-attacks.

[81] *AT&T Cybersecurity Insights: The CEO's Guide to Navigating the Threat Landscape*, AT&T, 2016, 28 s. Saatavissa (viitattu 24.5.2017): https://www.business.att.com/cybersecurity/docs/vol4-threatlandscape.pdf.

[82] C. Cerrudo and L. Apa, *Hacking Robots Before Skynet*, IOActive, 2017, 17 s. Saatavissa (viitattu 24.5.2017): https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf.

[83] *How the Internet of Things will affect security & privacy*, Business Insider, 2016, Saatavissa (viitattu 24.5.2017): http://www.businessinsider.com/internet-of-things-security-privacy-2016-8?IR=T.

[84] *Report on Workshop on Security & Privacy in IoT*, European Commission, AIOTI, 2017, 10 s. Saatavissa (viitattu 24.5.2017): http://www.theinternetofthings.eu/aioti-report-workshop-security-privacy-iot.

[85] *Security and Privacy Guidelines for the Internet of Things*, Schneier on Security, 2017, Saatavissa (viitattu 24.5.2017): https://www.schneier.com/blog/archives/2017/02/security_and_pr.html.

[86] *Toisille vaikeaa, toisille helppoa - käsitykset sähköpostihuijausten torjunnasta levällään*, Tivi, 2016, Saatavissa (viitattu 24.5.2017): http://www.tivi.fi/Kaikki_uutiset/ toisille-vaikeaa-toisille-helppoa-kasitykset-sahkopostihuijausten-torjunnasta-levallaan-6588201.

[87] T. Rintanen, *Asiantuntija: Suomessa vakoillaan erityisesti innovaatioita*, YLE, 2016, Saatavissa (viitattu 24.5.2017): http://yle.fi/uutiset/3-8988167.

[88] B. Gertz, *China cyber espionage continues*, The Washington Times, 2016, Saatavissa (viitattu 24.5.2017): http://www.washingtontimes.com/news/2016/sep/28/china-cyber-espionage-continues/.

[89] *2016 Manufacturing Report*, Sikich, 2016, 9 s. Saatavissa (viitattu 24.5.2017): http://www.sikich.com/insights-resources/thought-leadership/whitepapers/manufacturing-report-2016.

[90] A. Leppänen, K. Linderborg, and J. Saarimäki, *Tietoverkkorikollisuuden tilannekuva*, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja, 2016, 37 s. .Saatavissa (viitattu 24.5.2017): http://tietokayttoon.fi/documents/10616/2009122/17_Tietoverkkorikollisuuden+tilannekuva.pdf/6ef911d2-cbe8-43bd-aafa-e10ed573f28a?version=1.0.

[91] H. Linturi, J. Linturi, and A. Rubin, *eDelfoi – metodievoluutiota verkossa*, Maanpuolustuskorkeakoulu, Taktiikan laitos, 2013, Saatavissa (viitattu 24.5.2017): https://metodix.fi/2014/11/26/edelfoi-metodievoluutiota-verkossa/.

[92] *Suojelupoliisin vuosikirja 2016*, Suojelupoliisi, 2017, 28 s. Saatavissa (viitattu 24.5.2017): http://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/72827_SUPO_2016_FIN.pdf?103dd69c7476d488.

# LIITE 1. VALMISTELUTYÖPAJAN OSALLISTUJAT

Valmistelutyöpajaan 4.11.2016 osallistuivat seuraavat Deloitten kyberturvallisuus-asiantuntijat:

- Alin, Petteri
- Carleciuc, Gabriela
- Herland, Kristian
- Hokkanen, Teemu
- Ingström, Lasse
- Jansson, Jörgen
- Kangas, Jarkko
- Kasanen, Hannu
- Kokkonen, Mika
- Koivula, Nina
- Lähdemaa, Niko
- Mellin, Tero
- Pajunen, Kimmo
- Uusitalo, Teemu

# LIITE 2. DELFOIN 1. KIERROKSEN KYSYMYSRUNKO

1. Johdanto

   Oma roolisi ja vastuusi organisaatiossasi?

   Oma kokemuksesi kyberturvallisuusalalta (vuosissa mitattuna)?

   Mitä mielestäsi on kyberturvallisuus?

2. Kyberturvallisuuden paikka organisaatiossa

   Kuinka tieto-/kyberturvallisuuden hallinnointi ja hoitaminen on vastuutettu ja vastuu jakautunut organisaatiossasi? Onko kyberturvallisuus IT:n vastuulla? Riskienhallinnan vastuulla? Oman tietoturvapäällikön (CISO) vastuulla? Toimitusjohtajan vastuulla? Tietohallintojohtajan vastuulla? Tietoturvatiimin vastuulla? (Montako henkilöä?) Onko tähän vastuunjakoon tulossa muutoksia seuraavan viiden vuoden aikana?

   Kyberturvasuunnitelmat:

   Onko organisaatiosi viisivuotisvisioon/-strategiaan sisällytetty kyberturvallisuusaiheita?

   Onko kyberturvallisuusaiheet osa organisaatiosi riskienhallintaa/ sisällytetty riskienhallintastrategiaan?

   Onko organisaatiollasi erillinen kyberturvallisuusvisio ja/tai -strategia?

   Jos on, niin milloin visio/strategia on päivitetty tai tarkistettu? Kuinka pitkälle visio/strategia ylettyy?

   Jos ei, niin näkisikö vision tai strategian luomisesta olevan hyötyä? Onko syytä, miksei ole tehty?

   Mitä organisaatiosi kyberturvallisuutta parantavia toimia on suunniteltu toteutettavan 5 vuoden sisällä? Onko näihin toimiin sitouduttu?

   Millaisia toimia tulisi toteuttaa, jotta organisaation liiketoiminta pysyy turvattuna? Mitkä toimet ovat tärkeimpiä?

   Millaisia esteitä kyberturvallisuuden toteutumiselle näkisit yrityksenne kohtaavan 5 vuoden sisällä? (ulkoisia/sisäisiä esteitä)

Henkilökunnan tietoisuus:

Onko kyberturvallisuus organisaatiossasi myös ylemmän johdon (tai hallituksen) asia? Miten tämä näkyy organisaation tulevaisuuden suunnitelmissa?

Kuinka kiinnostunut organisaation ylin johto on kyberturvallisuusaiheista? Näetkö, että kiinnostus tulee vähentymään vai lisääntymään (vai pysymään ennallaan) lähitulevaisuudessa ja 5v päästä?

Ymmärtääkö yrityksen henkilökunta kyberturvallisuuden arvon liiketoiminnalle? (Nähdäänkö kyber-/tietoturvallisuus lähinnä liiketoiminnan hidastajana vai osataanko se nähdä myös mahdollistajana?)

Onko yrityksen suunnitelmissa muuttaa organisaation kyberturvallisuuskulttuuria ja henkilökunnan asenteita?

Aiotaanko työntekijöiden tietoturvakoulutusta lisätä tai vähentää tulevaisuudessa (5v sisällä)?

Kuinka hyvin yrityksesi keskeiset kyberturvallisuustoimijat ymmärtävät yrityksen ydinliiketoimintaa?

3. Investoinnit kyberturvallisuuteen

   Paljonko suhteessa muihin investointeihin organisaatiossasi on tällä hetkellä investoitu kyberturvallisuuteen (kyberuhkiin varautumiseen, niiden tunnistamiseen ja niiltä suojautumiseen)? Kyberturvallisuuteen on investoitu selvästi vähemmän kuin muualle / Kyberturvallisuuteen on investoitu enemmän kuin muualle / Kyberturvallisuuteen on investoitu yhtä paljon kuin organisaation muuhunkin toimintaan / Kyberturvallisuuteen ei ole investoitu oikeastaan ollenkaan

   Paljonko suhteessa muihin investointeihin organisaatiossasi tullaan tulevaisuudessa (5 vuoden aikana) investoimaan kyberturvallisuuteen? Kyberturvallisuuteen tullaan investoimaan selvästi vähemmän kuin muualle / Kyberturvallisuuteen tullaan investoimaan enemmän kuin muualle / Kyberturvallisuuteen tullaan investoimaan yhtä paljon kuin organisaation muuhunkin toimintaan / Kyberturvallisuuteen ei tulla investoimaan oikeastaan ollenkaan

   Mitataanko investointien tehokkuutta jotenkin?

   Miten investoinnit suhteessa jakautuvat kyberturvallisuuden sisällä tällä hetkellä/ 5v aikana? Miksi? Tekniset ratkaisut - Ohjelmistot ja prosessit - Henkilöstön osaaminen - Ulkoistaminen.

Mihin näet, että yrityksesi tulisi investoida seuraavan viiden vuoden aikana parantaakseen kyberturvallisuuttaan?

Henkilöstö: Ovatko henkilöstöresurssit organisaatiossasi riittäviä tällä hetkellä ja tullaanko samanlaisilla resursseilla pärjäämään myös viiden vuoden päästä?

Ohjelmistot ja prosessit: Millä tavalla hallinnoitte kyberturvallisuutta (ja sen osalta syntyviä tietoja)? Käytättekö kyberturvallisuuden hallinnassa jotain työkaluja? Jos kyllä, niin mitä? Oletteko aikeissa ostaa jonkin työkalun kyberturvallisuuden hallintaan seuraavan 5 vuoden aikana? Esim. Kokonaisvaltaista (GRC) ohjelmistoa, jonne syötetään tietoa muista ohjelmista (esim. SIEM, IDS/IPS...) ja sitä käytetään mm. riskien ja vaatimustenmukaisuuden hallinnassa sekä raportoinnissa ylimmälle johdolle. Esim. riskienhallinnan työkaluja (Granite, 4KS...), joista saadaan tietoa kyberturvallisuuden uhkaympäristöstä.

4. Tulevaisuudennäkymät vuoteen 2021

   Millaisena näet seuraavien toimijoiden näkökulmasta kyberturvallisuuden tulevaisuuden (5v päähän)? 1) suomalaisen valmistavan teollisuuden 2) oman organisaatiosi

   Mitkä ovat mielestäsi vuonna 2021 merkittävimmät omaa organisaatiotanne sekä yleisesti suomalaisen valmistavan teollisuutta koskevat kyberuhkat?

   Kuinka todennäköisenä pidät sitä, että organisaatiosi maine on uhattuna kyberhyökkäyksen takia seuraavan viiden vuoden aikana? Miksi? Erittäin todennäköisenä - Mahdollisena - Pieni mahdollisuus - Ei ollenkaan todennäköistä.

   Uskotko, että organisaatiosi kyberturvallisuudenhallinta on paremmalla, samalla vai heikommalla tasolla kuin muiden suomalaisten valmistavan teollisuuden yrityksien?

5. Kuka hyökkää ja miksi

   Ketkä voivat vaarantaa yrityksen kyberturvallisuuden 5 vuoden päästä? Keitä yrityksen tiedot voisivat kiinnostaa? Kilpailijoita? Valtiollisia toimijoita? Hackitivisteja? Ammattirikollisia? Miksi yrityksen tiedot kiinnostaisivat juuri tätä hyökkääjätyyppiä?

   Mikä yrityksessä kiinnostaa hyökkääjiä tai ulkopuolisia tahoja nyt/vuonna 2021? Esim. Taloustiedot, Asiakastiedot, Markkinointitiedot, Henkilöstötiedot, Maineriskiä aiheuttavien tietojen vuotaminen, esim. PII datan löytäminen, tuotekehitys- ja tutkimusdata, Pääseminen organisaation sisäverkkoon ja

IoT-laitteisiin aiheuttamaan tuhoja, Yrityksen tuotteista tietoturva-aukkojen etsiminen ja hyödyntäminen, jolloin vahinkoa myös loppuasiakkaalle, Hacktivismi ja kansallinen levottomuus.

# LIITE 3. ASIANTUNTIJAPANEELI

Tämän tutkimuksen delfoi-asiantuntijapaneeliin kuuluivat seuraavat henkilöt:

- Janne Puustinen, Vice President Information Technology, Valmet
- Jari Österberg, Head of IT Risk and Information Security Management, UPM
- Juho Rikala, Information Security Director, Fazer Oyj
- Kari Mikkola, IT Security and Risk Manager, Metso
- Kim Eklund, General Manager, Cyber Security, Quality, Wärtsilä Oyj
- Petteri Rantanen, Chief Security Officer, Nokia Oyj
- Sinikka Salmi, Manager IT Security and Compliance, Valtra/AGCO
- Tero Lampiluoto, Chief Information Security Officer, Outokumpu Oyj
- Tomi Pitkänen, Head of ICT Security, Neste Oyj

# LIITE 4. VÄITTÄMIÄ DELFOIN 1. KIERROKSELTA

Miksi

- Ongelmia syntyy, kun halutaan yhdistää vanha suljettu järjestelmä internetiin.
- Kyberturva on osa-alue, jossa jos liikut hitaasti, niin suhteellisesti liikut taaksepäin.
- Usein kysytään mitä tietoturva maksaa - pitäisi kysyä mitä maksaa toimimaton tunti?
- Asiakkaat tulevat kyllä kysymään, voiko yritykseemme luottaa ja tämä tarvitsee heille jotenkin todistaa.

Mitä

- "If it works, don't fix it" -malli ei ole enää tätä päivää.
- Täytyy tietää mitä suojelee, siitä kaikki lähtee.
- Mediassa lumipallo lähtee vyörymään helposti.
- Valmistavan teollisuuden kyberuhkakartalla on ja tulee olemaan paitsi kaikki normaalit uhkat niin myös monimutkainen tuotantoympäristö logiikkalaitteineen ja tuotteineen.

Miten

- Yksi koko ei enää istu kaikille.
- Tietoturvalla ei saa kiusata – on huomioitava ihmiset.
- Turvallisuusvaatimus täytyy integroitua kaikkeen tekemiseen.
- Onko kilpailijoilla mahdollisuus verkostoitua kyberturvallisuusasioissa?
- Ei tietoturvaprojekteja - vain liiketoiminnan projekteja, joissa tietoturva mukana.

# LIITE 5. VAIKUTTAA SUOMEN VALMISTAVAN TEOLLISUUDEN KYBERTURVALLISUUTEEN V.2021

Alla oleva listaan on koottu asiat ja trendit, jotka delfoin ensimmäisen kierroksen haastatteluissa panelistit mainitsivat useampaan kertaan Suomen valmistavan teollisuuden kyberturvallisuuteen vuonna 2021 vaikuttavina asioina.

- IoT ja digitalisoituminen
- automaation turvallisuus
- tietosuoja
- ylimmän johdon sitoutuminen ja sitouttaminen kriittistä
- kyberturvakulttuuri/ henkilöstön osaaminen
- kyberturvallisuuden mittaaminen
- saatavuuden varmistaminen
- kolmansien osapuolien kyberturvallisuuden taso ja hallinnointi
- kohdistetut hyökkäykset
- henkilöresurssien riittävyys
- huijaukset
- datan säilytys organisoidusti
- oikeat työkalut kyberturvallisuuden hallintaan
- kybervakoilu
- kyberturvaviestintä sisäisesti ja ulkoisesti
- maineriskien hallinta
- sosiaalinen media (mm. maineriskit)

- pilviturvallisuus
- identiteettien ja pääsynhallinta
- identiteettivarkaudet
- eri maiden erilaiset lait
- nopeat poliittiset muutokset ja muutokset toimintaympäristössä
- vanhojen järjestelmien turva-aukot
- kiristys ja terrorismi
- käytettävyys vs. tietoturva
- data-analytiikka ja BigDatan hyödyntäminen
- mobiililaitteet
- koko organisaation kattavien toimintatapojen ja vision toteutus
- sisäisten uhkien hallinta
- viranomaisyhteistyön haasteet
- järjestelmien kompleksisuus ja monimuotoisuus

# LIITE 6. JOITAKIN TOIMENPIDESUOSITUKSIA KIRJALLISUUDESTA

Erikoisraportissaan *Suojaamattomien automaatiolaitteiden kartoitus 2016* [54] Viestintävirasto antaa seuraavat suositukset teollisuuden tietoturvan parantamiseksi:

1) Tunne ympäristösi ja sen laitteet. Yritysten ja teollisuuden ulkorajapintoja on suositeltavaa kartoittaa säännöllisesti. Tällöin esimerkiksi vahingossa internetiin avoinna olevat palvelut huomataan ja järjestelmän turvallisuuden tilanne tulee kartoitettua. Jos kartoituksen tekee ulkopuolinen, näkökulma voi erota oman henkilökunnan näkökulmasta, ja siten on mahdollista saada entistä monipuolisempi näkemys tilanteesta. Huomioi, että automaatioympäristön käytönaikainen skannaaminen automaatioverkossa ei ole järkevää vaan on tehtävä suunnitelmallisesti huoltokatkosten yhteydessä.

2) Säännöllisellä yrityksen verkon tutkimuksella havaitaan myös, onko palveluihin kohdistuneiden haavoittuvuuksien korjaaminen onnistunut, toimivatko päivitysprosessit ja onko verkko suunnitellun mukainen.

Artikkeli *Secure Information Sharing in an Industrial Internet of Things* [56, s. 9-10] taas suosittelee IIoT:n suojaamiseen seuraavia, lyhyellä tähtäimellä mahdollisia, parhaita käytäntöjä:

1) Verkon segmentointi

2) Jatkuva monitorointi ja analysointi

3) Lokien analysointi

4) Tiedostojen eheyden seuranta

5) Verkon liikenteen seuranta

6) Muistivedosten ja varmuuskopioiden analysointi

7) Tavalliset työkalut haitallisen toiminnan tunnistamiseen

8) Jatkuva päivittäminen ja tietoturva-aukkojen paikkaaminen (patching)

9) Säännöllinen haavoittuvuustestaus

10) Proxy-ratkaisut

# LIITE 7. EHDOTUKSIA TUTKIMUSKYSYMYKSIKSI JATKOTUTKIMUKSIIN

Muun muassa tämän tutkimuksen alkuselvityksen omaisesta luonteesta johtuen jäi tutkimuksen jälkeen paljon aiheita, joita tulee tulevaisuudessa tutkia tarkemmin. Tulevaisuuden tutkimyuskysymyksiä suoralle jatkotutkimuskelle eli tavallaan delfoin kolmannelle kierrokselle voisivat olla esimerkiksi:

- Miksi identiteettivarkauksia ei koeta tulevaisuudessa tärkeäksi Suomen valmistavan teollisuuden kyberturvallisuudelle, vaikka identiteettien ja pääsynhallinta koetaan?
- Mitä tärkeiksi tunnistettujen asioiden eteen on kussakin yrityksessä suunnitelmissa tehdä ja miksi?
- Mahdollisesti Suomen valmistavan teollisuuden kyberturvallisuudelle tärkeät asiat: miksi tietyt panelistit väkivät ne tärkeinä ja toiset vähemmän tärkeinä? Miksi joitakin asioita yksikään panelisteista ei nostanut erityisesti esille? Mistä ristiriidat näiden asioiden kohdalla aiheutuivat? Mikä näiden asioiden merkitys tulee olemaan tulevaisuudessa?
- Kuinka hyvin valmistava teollisuus valmistautunut tutkimuksessa tunnistettuihin tulevaisuudenkuviin?
- Kuinka kyberturvalisuusinvestointeja voisi mitata?
- Mikä lasketaan kyberturvallisuusinvestoinniksi?
- Kuinka valmistavan teollisuuden yrityksen olisi mahdollista saada kokonaisvaltainen näkemys investointiensa tehokkuuteen?
- Toteutuivatko tutkimuksessa annetut ennusteet vuonna 2021 ja miksi?
- Näkeekö Suomen valmistava teollisuus kyberturvallisuuteen panostamisen tulevaisuudessakin lähinnä vain kustannuksena vai osataanko se nähdä myös investointina? Olisiko tätä asennetta mahdollista muuttaa?

- Kuinka eri tavoilla eri toimialat määrittelevät kyberturvallisuuden? Mistä erot johtuvat?
- Mitkä ovat Suomen valmistavan teollisuuden yrityksissä kyberturvallisuuden tavoitteet ja mitä suunnitelmia niiden saavuttamiseksi on tehty?